“I don’t understand it”

A critical evaluation of how the Isle of Man public perceive cybercrime.

Laura Perkins.

UCM
University College Isle of Man
Colleish-Ollooscoill, Ellan Vannin
a College of Further & Higher Education

Overview

- Background and Motivation
- What is Cybercrime?
  - Example definitions
  - Accepted definitions
- Associated Fears
  - Example fears
  - Emerging themes
- Data Analysis
  - Thematic Analysis
  - Inferential Statistics
- Looking Forward
  - What can we do?

Background and Motivation

Background

- Keen interest in cybercrime and its consequences.
- Working in cybersecurity outside of the degree has highlighted a lack of awareness into cybercrime.
- Similar research has been carried out elsewhere but not on the Isle of Man.
- Do Manx residents understand cybercrime, and where can we improve?

Testable Hypothesis

"A lack of understanding into cybercrime as an entity has altered the fears of different groups of Isle of Man residents."

What is “Cybercrime”?

Respondent Definitions

During the research phase of the project a survey was carried out to try and gauge the level of understanding Manx residents have of cybercrime as an entity.

- “Having my personal details including financial information 'stolen', possibly by stealth, to be used without my knowledge and/or agreement.”
- “Using technology to commit a crime ie data theft fraud scams etc”
- “Online scams, mostly comments on Facebook giveaways. Phishing links are a common one. Identity theft, hacking, viruses.”
- “computer viruses and fraud.”
- “breaches - for money or to disrupt things”
- “Using technology, in particular online technology to assist in a crime that may also contain elements of "traditional" crimes”
- “Any form of extortion or scamming done through an online platform or link”
- “doesn’t interest me. I feel like it’s inevitable in this day and age”

Accepted Definitions

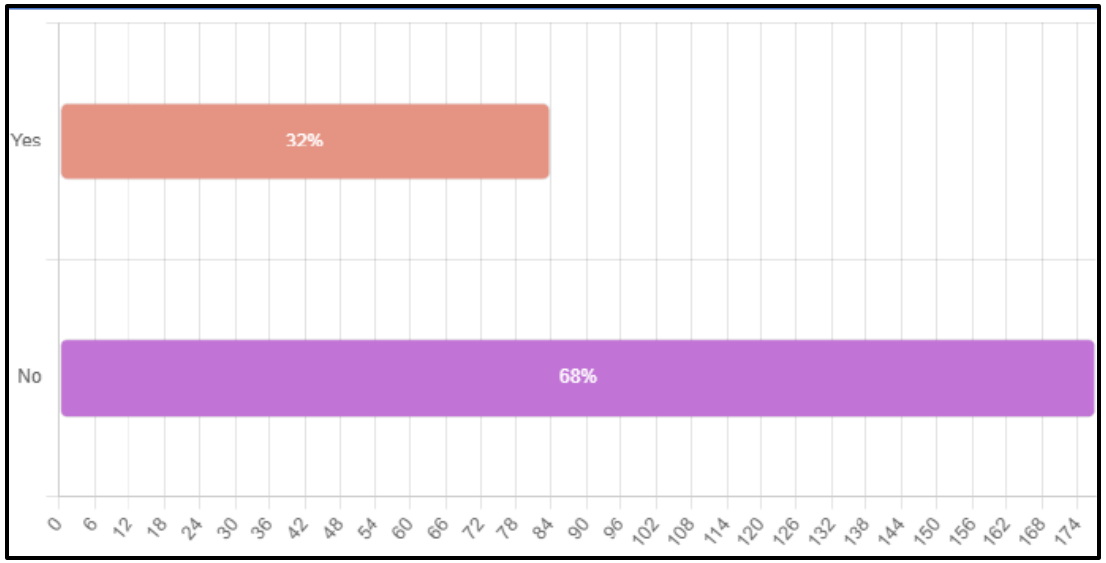
The accepted definition for cybercrime comes from the NCSC, and can be broken down into two subcategories:

- Cyber-dependent
- Cyber-enabled

- Cyber-dependent crimes - crimes that can be committed only using Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
- Cyber-enabled crimes - traditional crimes which can be increased in scale or reach using computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

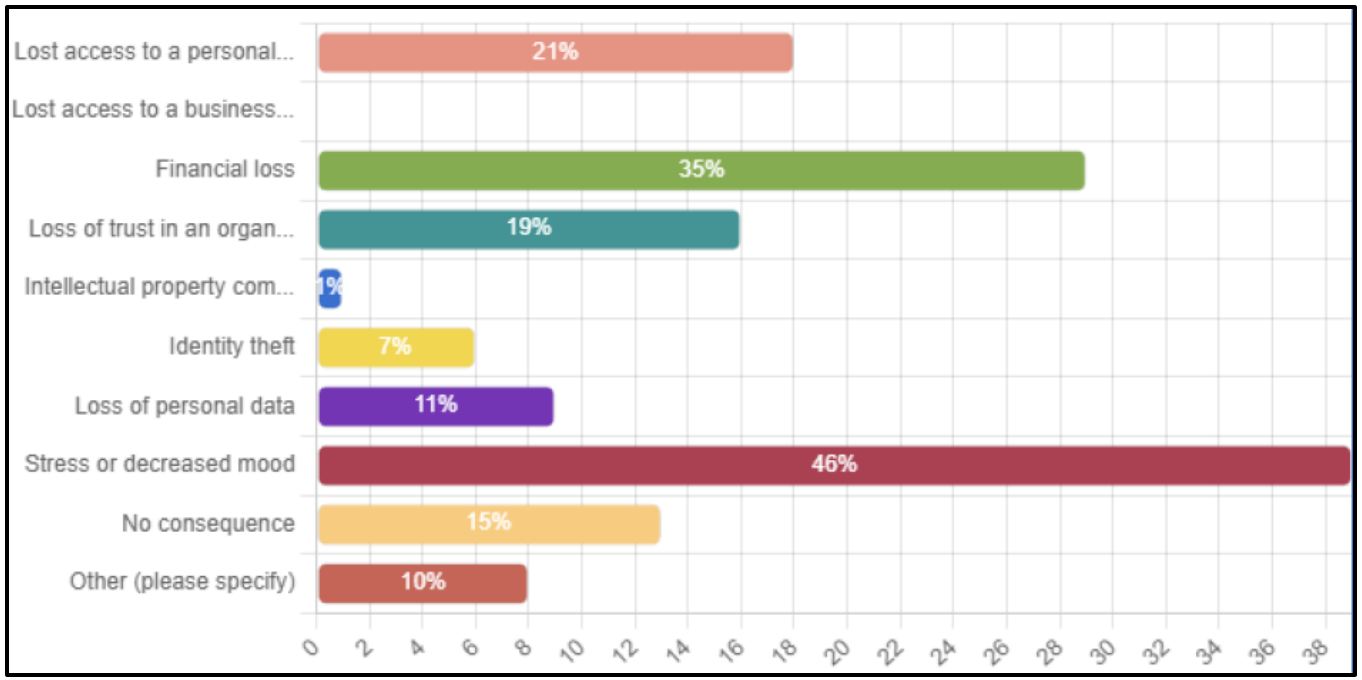
How Common is Cybercrime on Island?

- Phishing, smishing and vishing
- Purchase scams (including those on places like Facebook Marketplace
- Malware or ransomware
- Sextortion or romance fraud
- Account compromise or account loss
- Gift card fraud
- Fake profiles or impersonation of an account
- Investment scams (including cryptocurrency scams)
- Business email compromise
- DoS/DDoS attacks



Cybercrime Consequences

- Lost access to a personal account
- Lost access to a business account
- Financial loss
- Lost trust in an organisation
- Intellectual property compromise
- Identity theft
- Loss of personal data
- Stress or decreased mood



Associated Fears

Respondent Fears

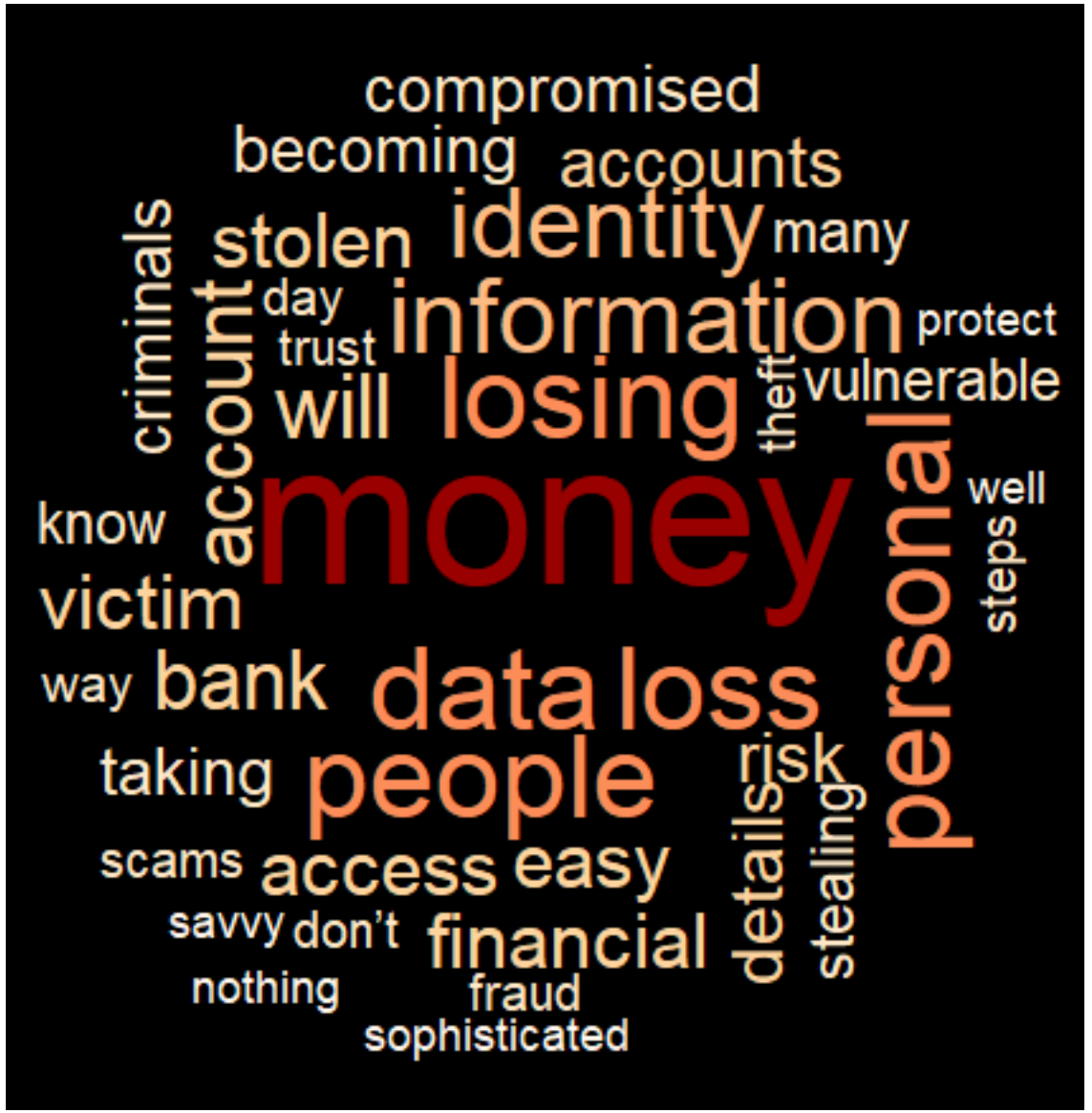
During the research phase of the project a survey was carried out to try and understand what Manx residents are scared of when they think about cybercrime.

- “How rapidly it changes and adapts/keeping ontop of it”
- “Access to bank details and private information, DOB etc”
- “That my personal information or bank account information may be obtained and misused by others and the potential financial impact, as well as the risk of identity theft.”
- “My children more than anything - where I may be careful, I worry that they aren't. More education within schools is definitely needed.”
- “Many scams are so sophisticated nowadays that despite being careful anyone can become a victim of cybercrime”
- “Cybercrime is becoming more sophisticated and harder to detect. I feel well versed in the warning signs to be aware of, but worry that less technologically aware users are more vulnerable to cybercrime. If I were to become a victim of cybercrime I would be worried about losing my money, with no recourse or ability to recover the funds.”

Emerging Themes

Respondents fear monetary loss the most, but this is closely followed by data loss.

Words like ‘vulnerable’ and ‘savvy’ were frequently used by respondents with the context that there is a fear arising from residents worried out those less technologically inclined falling victim.



Data Analysis

Thematic Analysis

- A popular method for analysing patterns in qualitative data.
- Themes have been identified from transcripts produced following on from focus groups.
- Thematic analysis has been used to examine the themes regarding cybercrime mitigation tactics for the future.

Initial Codes and Themes

Theme	Code		
Password protection	“strong passwords”	“changing passwords regularly”	“avoid reusing passwords”
Awareness and Vigilance	“be aware of financial transactions”	“verify transactions”	“be cautious about phishing emails”
Technical Measures	“using VPNs”	“minimising information put online”	“using guest checkouts”
Critical Thinking	“verify emails from banks”	“be cautious about clicking on links”	“check your privacy settings”
Data Privacy	“manage privacy settings on social media”	“understand the implications of posting stuff online”	

Final Report

Theme	Highlighted Information
Password protection	Participants emphasised the importance of having strong passwords, changing them regularly, and avoiding password reuse to protect against cyber threats.
Awareness and Vigilance	Participants highlighted the need to stay vigilant and aware of potential cyber threats, such as suspicious charges or phishing emails.
Technical Measures	Participants mentioned various technical measures and tools aimed at enhancing online privacy and security, such as using VPNs and minimising the disclosure of personal information online.
Critical Thinking	Participants stressed the importance of critical thinking and verification when encountering suspicious emails or links, as well as verifying the authenticity of communications from financial institutions.
Data Privacy	Participants discussed managing privacy settings on social media platforms and being cautious about the information shared online to prevent identity theft or data breaches.

Analysis of Variance

- Statistical technique used for analysing variation.
- Survey respondents split up and categorized based on how easy they find technology to use.
- “There is no significant difference in word frequencies among individuals who find technology easy to use, difficult to use, or have no opinion on ease of use”.

Initial Codes and Themes

To carry out this analysis the collected data was input into R Studio and the statistical programming language ‘R’ was used.

The data was added to a corpus (data set) and cleaned to remove filler words, punctuation, blank spaces, and numbers.

If you would like to see the code, please do ask and I am more than happy to send it to you.

	Degrees of Freedom	Sum of Squares	Mean of Squares
Group	2	73	36.67
Residuals	501	4044	8.07

Based on the table, it can be concluded that there is a significant statistical difference between the three tested groups at the 0.05 level.

Looking Forward

What Can We Do?

- Provide more training.
- Increase the awareness of cybercrime on Island.
- Stay vigilant online.
- Local Support – Cyber Security Centre for the IOM

Thank You.

Laura Perkins

UCM
University College Isle of Man
Colleish-Ollooscoill, Ellan Vannin
a College of Further & Higher Education