Gwasanaeth Tân ac Achub De Cymru

South Wales Fire and Rescue Service

DATE: 13 August 2018 **FOI REQUEST NO: 104_1819**

I am writing to make a request for information under the Freedom of Information Act 2000.

If this request is too wide or unclear, I would be grateful if you could contact me as I understand that under the Act, you are required to advise and assist requesters. If any of this information is already in the public domain, please can you direct me to it, with page references and URLs if necessary.

I understand that you are required to respond to my request within the 20 working days after you receive this letter.

Q. What percentage of emails that your organisation receives are fraudulent – i.e. phishing messages, BEC (business email compromise) attacks, CEO Fraud, malware laden, etc.

Please see Appendix A

Q. What is the most common type of fraudulent email/cyber-attack that your organisation receives?

- CEO fraud – this is when someone sends an email impersonating a senior company executive asking an employee to make payments for goods or services into a fraudulent bank account
- Fraudulent transaction requests – fraudsters send invoices for payment of goods or services as if from a legitimate organisation – **This is the most common type of attack vector as some get past our grey-listing checks; especially of late, and I block the domains on an ad-hoc basis.**

- Credential theft – fraudsters send messages trying to get users to divulge their username and password or other sensitive information
- Ransomware
- Other
- Don't Track

Q. Has your organisation suffered financial loss in the last 12 months as a direct result of a faked email message being received that tricked an employee into sending money via wire transfer

- Yes
- **No**

If yes, please state how much was lost (if fallen victim more than once, please provide total amount given to scammers): _____

Q. Has your organisation had a device/system infected by ransomware in the last 12 months that was delivered via email:

- Yes – once
- Yes – more than once
- We were infected by ransomware but the source wasn't traced
- **Never**

NB: If you have answered yes, please answer the following questions for each separate ransomware infection (if numerous devices were infected at the same time, this counts as one incident)

How long were systems affected: _____

Did you pay the ransom:

- Yes
- No

If yes, how much was paid: _____

Did the criminals provide the information/program needed to restore systems:

- Yes
- No

Q. Do you use the domain-based message authentication, reporting and conformance protocol (DMARC) to block fake emails being spoofed to appear as if they have been sent by your company/organisation:

- Yes
- **No - in the process of implementing this**
- Don't know

Q. Are you aware if your organisation/brand has ever been 'spoofed' and used by scammers to send emails trying to trick people

- Yes – before we started using DMARC
- Yes – after we started using DMARC
- Yes – but not sure if it was before or after using DMARC
- Never
- **Don't Track**

If yes, please state how many separate incidents of your organisation/brand being spoofed that you know of:

before we started using DMARC: _____

after we started using DMARC: _____

Q. Do you publicise externally how a member of the public can check an email communication with your organisation to determine if it is fake?

- Yes
- **No – we do provide this information to selected partners**

If yes, how many reports have you received in the last 6 months of fake/phishing messages:

- _____

- **Don't Track**

Q. Do you publicise internally how a member of your workforce (including third party suppliers) can check an email communication with your IT/Security team to determine if it is fake?

- **Yes**
- No

If yes, how many reports have you received in the last 6 months of fake/phishing messages:

- _____ from internal workforce

- _____ from third party suppliers

- _____ from both internal and third party suppliers as don't differentiate between senders

- **Don't Track**

Q. Do you provide a report button within your email system for end users to report phishing emails?

- Yes
- **No**

Q. Does your organisation have a SOC (Security Operations Centre) or IT security team?

- Yes
- **No**

Q. Do you have a secure email gateway?

- **Yes**
- No
- Don't know

Appendix A

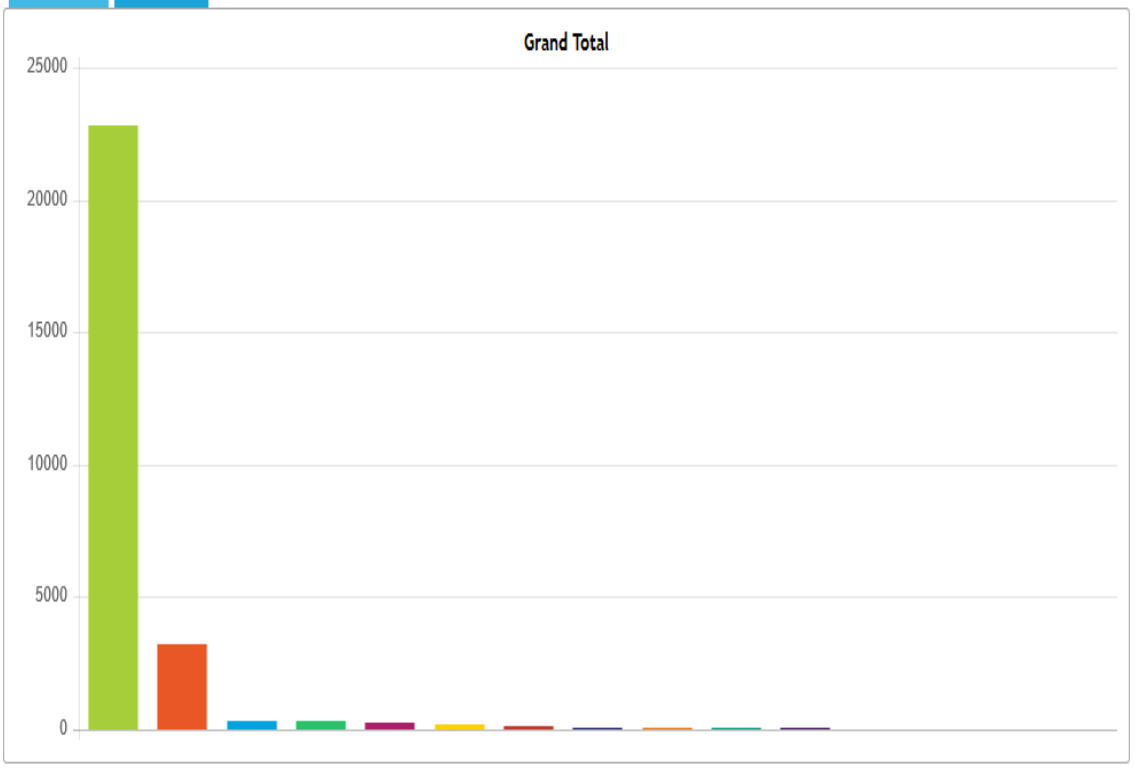
In the local reporting database:

The summary data spans the period from 2018-04-11 to 2018-07-10.

The detailed data spans the period from 2018-06-10 to 2018-07-10.

Held Area : **Any**

Msg Counts | Msg Volume



Held Area	Msg Count	Msg Volume
Spam	22831	958.3 MB
Active Content	3246	809.7 MB
Profanity	354	878.0 MB
Blocked Recipients	351	199.1 MB
Encrypted	251	462.6 MB
ZIP Files	219	810.2 MB
Misrouted Messages	134	757 KB
Executables	79	310.0 MB
Multimedia	73	908.0 MB
Virus	58	31.8 MB
Blocked Senders	42	51.5 MB
Secure Portal Informs	20	93 KB
Message Processing Failure	19	81.4 MB
Parked	15	1.0 GB
Oversize	2	198.3 MB

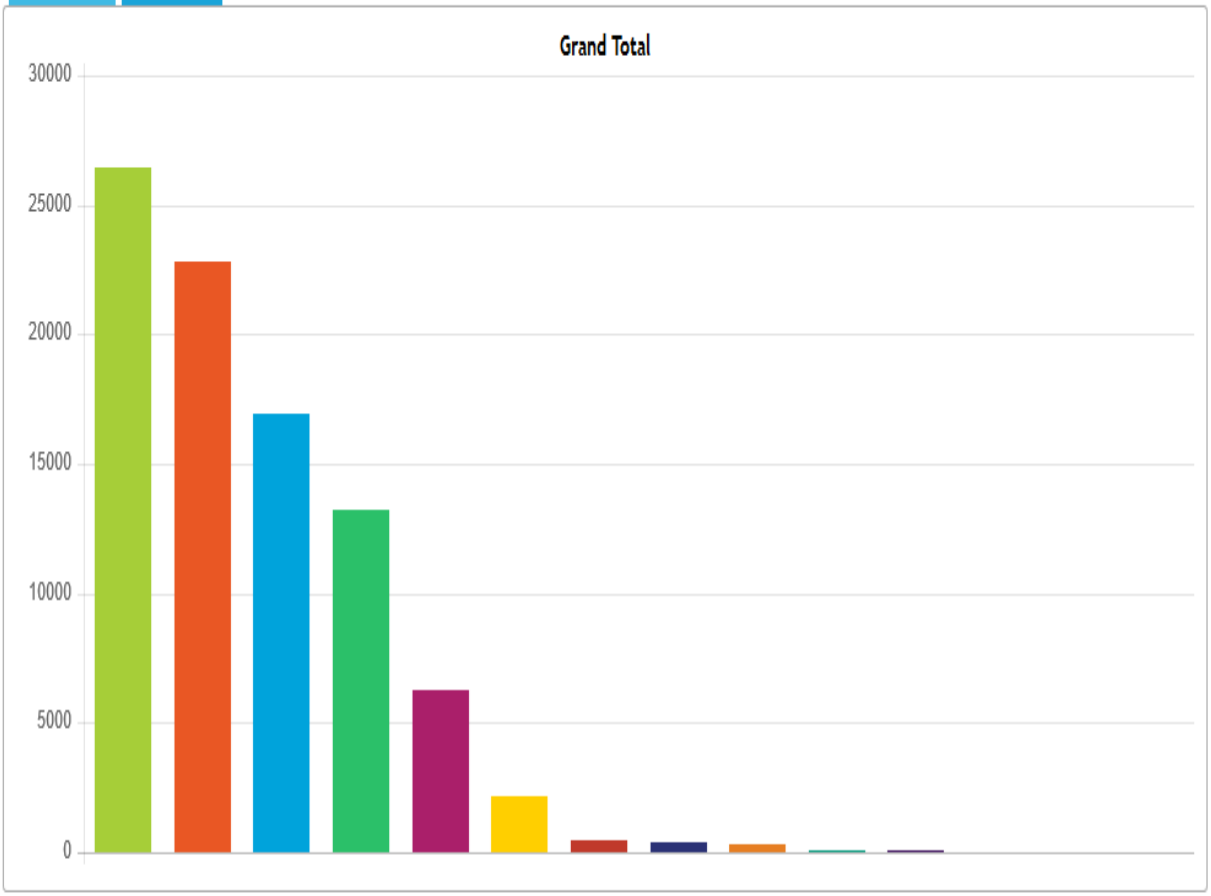
Date Range : **This Year (2018-01-01 00:00:00 - 2018-07-12 00:00:00)**

In the local reporting database:

The summary data spans the period from 2018-04-11 to 2018-07-10.

The detailed data spans the period from 2018-06-10 to 2018-07-10.

Msg Counts | Msg Volume



Threat Description	Msg Count	Msg Volume
Bad Reputation	26468	0 B
Junk Email Detection	22814	958.9 MB
Domain of sender address does not exist	16915	0 B
Real-time Blacklist	13194	0 B
Banned sender	6249	0 B
DKIM Hard Fail	2178	579.5 MB
SPF fail	441	0 B
Relaying denied	386	0 B
DMARC Reject	274	16.2 MB
DMARC Quarantine	103	4.0 MB
Sender spoofed	49	0 B
Phishing	19	754 KB
Other reject reason	12	0 B
Recipient verification	1	0 B

Time to execute report: 338 ms