What are the metrics that exist in practice?

In practice, most metrics are not so specific as in an ideal situation. They do not discriminate between business sectors, amount of internet users per area, and so on. It is obvious that the main goal of phishing information clearinghouses, like phishtank.com, is merely to expose phishing sites. Although sometimes it is possible to search for certain variables such as “target” and “country”, performance variables such as uptime are not kept track of. It is therefore hard to retrieve an extensive database from which research can be conducted.

The variables, and therefore the conductable metrics, of phishing detection sites are based on incidents. They are hard to interpret without knowledge of underlying, sometimes hidden, causal relationships. The examples below are incomplete in that sense, since normalisation or underlying causalities are not taken into account.

Although no useful conclusions can be derived from these metrics, it does show that these phishing clearinghouses focus on measuring the prevalence and severity of phishing sites.

PhishTank.com (2015) and Clean MX (2015) deliver data on the following statistics:

|  |  |
| --- | --- |
| PhishTank | Clean MX |
| * Phishes Verified per Day * Phishes Submitted per Day and per Hour * Total Phishes Submitted / Valid / Invalid per month * Median Time to Verify (by the community) * Top 10 domains of valid phishes * Top 10 IP adresses of valid phishes * Top 10 Networks that host phishes * Popular Targets | * Phishes detected and closed per Day * Distribution of % phishing sites worldwide and per country * Nameserver distribution worldwide and per top 25 countries * Phishingsite distribution top 25 countries, per region |

Apart from the above examples of incomplete incident metrics, another phishing related type of metric is found in literature. This is about how well a technology is capable of recognizing phishing sites or e-mails. These metrics are based on controls and their performance.

Searching in databases like Scopus and IEEE with search terms “phishing” and “metric\*”only deliver one page with results – which is not much. When “metric\*” is left out, suddenly over 5 pages of results come up. This might indicate a lack of experience and performance evaluation in phishing management.

An interesting question is how the submitted phishing sites were detected. Is it because of excellent technological systems, or because of high employee awareness?

References

DeBarr, D., Ramanathan, V., & Wechsler, H. (2013). Phishing Detection Using Traffic Behaviour, Spectral Clustering, and Random Forests. *Proceedings of* *ISI 2013, June 4-7, 2013, Seattle, Washington, USA.*

*\*\* 4 more articles to be referenced \*\**

Clean MX (2015). *Phish Stats.* Retrieved on September 15 via <http://support.clean-mx.de/clean-mx/phishstats>

PhishTank.com (2015). *Stats*. Retrieved on September 15 via <http://www.phishtank.com/stats.php>

NoticeBored (2008). *Management Briefing on Authentication and Phishing Metrics.*Retrieved from http://www.securitymetametrics.com/61\_NB\_mgmt\_briefing\_on\_phishing\_metrics.pdf on September 9, 2015.

* Number of authentication failures
* Proportion of authentication failures
* Authentication trends
* Authentication confidence level
* Phishing detection and response rates (time between launch & detection, and detection & removal)