Natural Language IAS: The Problem of Phishing

Students: Lauren M. Stuart, Gilchan Park. Advisors: Prof. Julia M. Taylor, Prof. Victor Raskin

Examples: snippets from actual phishing emails\(^1\), with Ontological Semantics Technology\(^2\) –based analysis.

Existing Strategies
Several proposed policies and implemented tools exist for separating likely phishing emails from legitimate emails.

- Blacklists/whitelists for domains and addresses\(^3\)
- Link analysis: target/text mismatch, features of common bad URLs\(^4,5\)
- Language analysis: common keywords, expanded language consideration\(^5,6,7\)
- Visual/DOM analysis: Page elements of fake and real login pages\(^5,8,9\)

Proposed Direction
Expand the use of linguistic semantics in information security.

- Quantify and/or canonize linguistic and logical hallmarks of phishing emails for detection
  Similar methods in stylometric analysis, automatic characterization of network events
- Semantic analysis of message content: comparisons and thresholds

Semantic analysis of message content:

Ontological Semantic Technology: semantic scripts, text meaning representation, fuzzy logic

Work/Compensation Mismatches
Phishing emails sometimes promise a great deal of money or benefits in return for seemingly little work in order to lure people into divulging sensitive information.

"The Washington Mutual Bank Online department kindly asks you to take part in our quick and easy 5 questions survey. In return we will credit $1000.00 to your account - Just for your time!"

Awkward/Unprofessional Phrasing
Though many professional, legitimate emails do have grammatical mistakes and awkward phrasing, it may pay to be more skeptical of an "official" communication that does have these mistakes.

"Why you become a PowerSeller?"
"If you agree, please within 24 hours."

Inconsistency with Company Policy
Some phishing emails directly contradict publicly-available company policies and can be fact-checked if presented as fact. Checking inconsistency in semantic structures is potentially complicated but one simplification of the idea could look like this:

"You have to click the highlighted fields below and in few days you will become an eBay power seller."

"You don't need to apply for the PowerSeller program. If you qualify, you'll automatically be included." (http://pages.ebay.com/help/sell/sell-powersellers.html)

References

Possible candidates for \(\approx\) function: human-set threshold, mined threshold, – but how to express proportionality?

Automatic Language Usage Analysis

ungrammatical or <30% acceptable
Parser-based verification is subject to false positives when language resources don't have 100% coverage. Non-binary results can give finer-grained control.

grammatical or >80% acceptable

Comparison against an authoritative source is common; in this case, semantic analysis allows for direct comparison of texts.