

1 RESEARCH GOALS

Research Question: Are certain visual phishing cues more identifiable than others, and are certain cues more likely to be ignored or not easily detected?

Initial study: Examination of the prevalence and frequency of cues in real-world phishing emails.

2 METHODOLOGY

Analyzed 59 publicly available real-world phishing emails from three Phish Bowls:

- Taft College
- Univ. of California, Santa Cruz
- Univ. of Vermont



3 NIST PHISH SCALE – Cues

Cue Type	Cue
Error	Spelling and grammar irregularities
	Inconsistency
Technical indicator	Attachment type
	Sender display name and email address
	URL hyperlinking
Visual presentation indicator	Domain spoofing
	No/minimal branding and logos
	Logo imitation or out-of-date branding/logos
Language and content	Unprofessional looking design or formatting
	Security indicators and icons
	Legal language/copyright info/disclaimers
	Distracting detail
	Requests for sensitive information
Common tactic	Sense of urgency
	Threatening language
	Generic greeting
	Lack of signer details
	Humanitarian appeals
	Too good to be true offers
	You're special
	Limited time offer
	Mimics a work or business process
	Poses as friend, colleague, supervisor, authority figure

4 RESULTS

Phishing email cue prevalence analysis

For these data, n=59.

Four out of five types of cues were present in **at least 90%** of the emails analyzed.

Prevalence of Cue Types		
Cue Type	Number of Emails	% of Emails
Language and Content	59	100.00%
Common tactic	58	98.31%
Technical indicator	56	94.92%
Errors	55	93.22%
Visual presentation indicator	33	55.93%

Six out of 23 cues were the most common among phishing emails, appearing in **more than 50%** of the emails.

Prevalence of Cues			
Cue	Cue Type	Number of Emails	% of Emails
Mimics a work or business process	Common tactic	54	91.53%
Poses as a friend, colleague, supervisor, authority figure	Common tactic	51	86.44%
Spelling and grammar irregularities	Errors	50	84.75%
Generic greeting	Language and content	47	79.66%
Domain spoofing	Technical indicator	43	72.88%
Lack of signer details	Language and content	36	61.02%

Phishing email cue frequency analysis

There were 754 total instances of cues across the 59 phishing emails. For these data, n=754 total cues.

Cues in the *Language and content* and *Error* cue types accounted for nearly **one-third** of the total cues.

Frequency of Cue Types		
Cue Type	Number of Instances	% of Instances
Language and content	232	30.77%
Errors	227	30.11%
Technical indicator	128	16.98%
Common tactic	110	14.59%
Visual presentation indicator	57	7.56%

Spelling and grammar irregularities accounted for more than **one-quarter** of the total cues (27.06%), with a wide gap to the cue that appeared next most (*Generic greeting*, 9.42%).

Frequency of Cues			
Cue	Cue Type	Number of Instances	% of Instances
Spelling and grammar irregularities	Errors	204	27.06%
Generic greeting	Language and content	71	9.42%
Domain Spoofing	Technical indicator	57	7.56%
Mimics a work or business process	Common tactic	54	7.16%
Poses as a friend, colleague, supervisor, authority figure	Common tactic	51	6.76%
Requests for sensitive information	Language and content	47	6.23%

5 CONCLUSION

Our findings provide a depiction of the prevalence and frequency of cues within real-world phishing emails from university phish bowls. We intend to use these findings to inform our larger study to investigate people's ability to identify different types of cues.