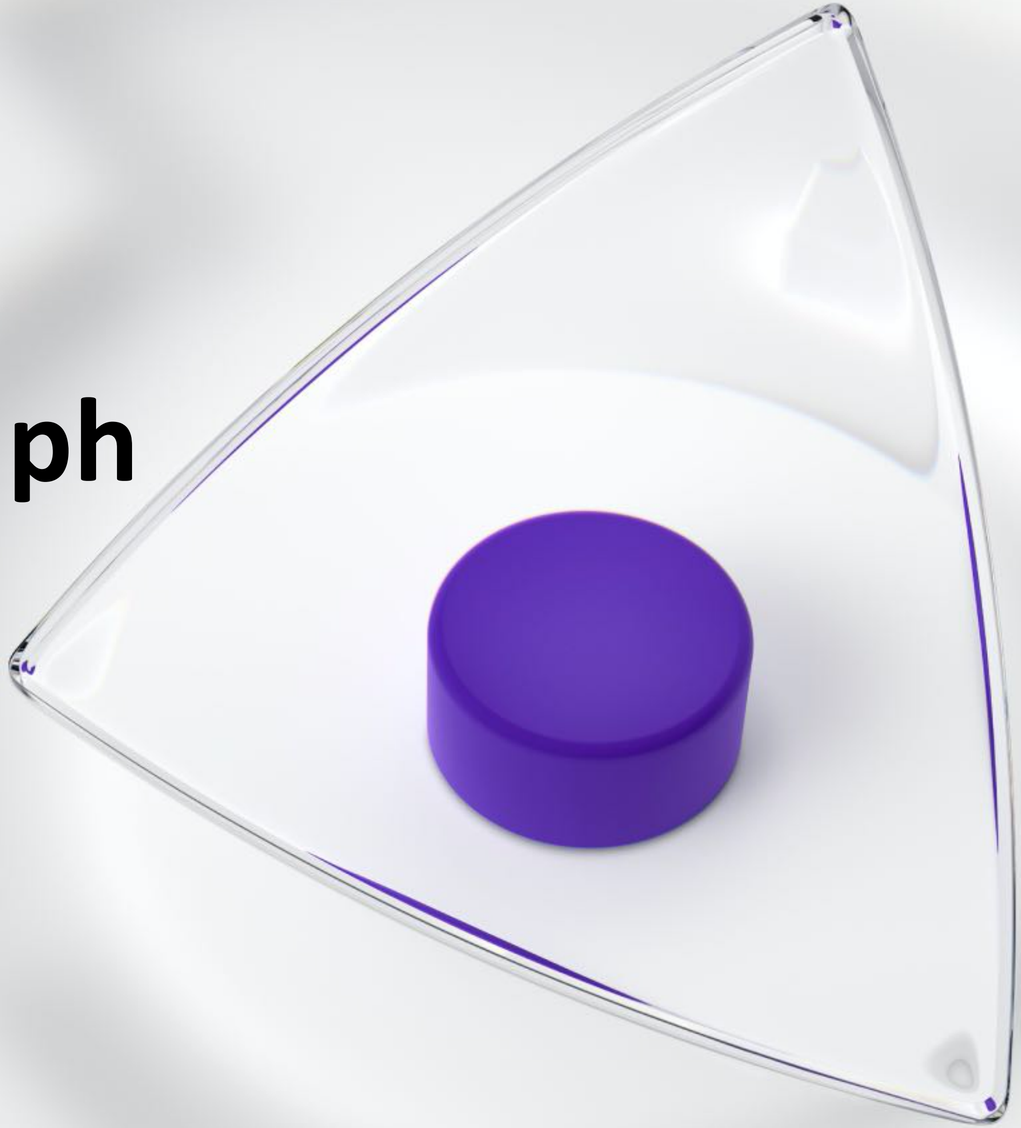
Clarivate
MarkMonitor™

Homoglyph/homograph domain names



Challenges and approaches

Brian King, MarkMonitor

Brian Lonergan, Donuts

Problem Summary

Problem Summary

brɑnd.com

brand.com

brand.com

br a nd.com

bra n d.com

brand.com

bran d .com

bran d .com

Ь r a n d .com

Problem Summary

brɑnd.com

brɑnd.com

brand.com

br a nd.com

bra n d.com

brand.com

bran d .com

bran d .com

b r a n d .com

Problem Summary

- google.domains
- google.domains
- gꝏgle.domains

- goog|e.domains
- google.domains
- gꝏgle.domains

Problem Summary

- xn--oogle-qmc.domains
  google.domains

- xn--gogle-m29a.domains
  google.domains

- xn--ggle-qk8o.domains
  gꝏgle.domains

- xn--googe-8tb.domains
  goog|e.domains

- xn--ogle-z7b4902b.domains
  google.domains

- xn--gle-8tb4222s.domains
  gꝏgle.domains

Complicating factors

Browsers may/not show punycode

-https://chromium.googlesource.com/chromium/src/+/master/docs/idn.md

Email clients may/not show punycode

Fonts may help, or not

Efforts to Address the Problem

Baseline

ICANN Guidelines for the Implementation of Internationalized Domain Names, version 3 (2011)

Unicode was the agreed standard for domain name characters

One script per domain, no comingling scripts

Whole-script confusables remain available for exploitation

Policy decisions in play today

Prohibit mixed script domains

-Baseline, required by ICANN

Require **language** instead of **script** indication

Block outright

-Bad policy, restricts legitimate use

Block variants/confusables after ASCII registration

Other options

-Remove select problematic confusables (https://www.soluble.ai/blog/public-disclosure-emoji-to-zero-day)

-L33t-sp3ak approach (UNR EPS block)

Scope of Problem

Scope

Homoglyphs are low **percentage** of phishing attacks

Interisle reports:

-219/298,000 phishing reports were IDNs, 0.2% of domains used

-50 classified as true homographic attacks; including:

-santąnder.com

-verízonwíreless.com

http://www.interisle.net/PhishingLandscape2020.pdf

- Overall effectiveness remains unknown
- Data needed on effectiveness of homoglyph attacks
- If good policy can stop just one, it’s worth it

Thank you

Thank you to Donuts, UNR, and Verisign for providing background, research, and insights.

Questions?

Clarivate™

Thank you!