livingsecurity

Successfully Delivering a Smish

Before launching a smishing campaign, it is important to launch test campaigns to bypass the sensitivities around an SMS.

Phone carrier + Type of phone

Security measures are in place for specific wireless carriers as well as both Androids and iPhones. The security measures fluctuate as much as day by day, so it is important to continuously test to ensure deliverability.

Text Message Content

To bypass spam filters, be wary of sensitive words or phrases that may trigger security measures. Big brand names or words like “login”, “accountid” can be marked as suspicious.

Phishing URL + Domain

URLs and domains including sensitive words like ‘verify’ or ‘password’, including mentions of big brands may also be identified as questionable. Test the domains Living Security offers or import your own domain.

Landing Page Content

The same logic applies with landing pages. Living Security’s landing pages are periodically tested for flagging, so the best practice is to duplicate Living Security's landing pages and make it your own, if there are customization needs.

SUMMARY

- Launch multiple test campaigns before the actual smishing campaign
- If allowed, toggle off any security measures placed.
- Review Sending Report and adjust accordingly
  - Start with text message content
  - If still Not Delivered, then test different URL domains, then test landing page content.

With Living Security

Living Security ensures to equip companies’ employees with the right tools to stay current and vigilant with modern attack vectors, such as smishing.

Additional technical support is available:
https://www.livingsecurity.com/support/contact-us

www.livingsecurity.com