SOLUTION BRIEF

INKY™
A Kaseya COMPANY

Maintaining Email Security in Google Workspace

Some organizations have chosen to use Google Workspace (formerly G Suite) for their integrated productivity packages. However, within Workspace, Gmail security continues to be a primary concern.

INKY Stops Phishing

INKY is cloud-based email protection software. It blocks spam, malware, and most importantly, phishing attacks.

User-Friendly Banners and Reporting Links

Computer Vision Brand Forgery Protection

User Profiling/ Social Network Mapping

No Software to Install/Risk Free

Workspace Security

Google employs Transport Layer Security (TLS) for messages in flight and strong encryption for messages at rest. These measures ensure the integrity of bits under Google's control.

Google can ascertain that no bits were changed between sender and recipient, but not whether the sender is reliable. Though it may pass all the tests, the email still may contain poisoned penmanship. A bad email may be sent from a legitimate but hacked account or the domain itself may have been spoofed. Google has enabled rudimentary phishing protection in Gmail, letting customers specify. Their own Sender Policy Framework (SPF) records and cryptographically mark email with Domain Keys Identified Mail (DKIM). But the effectiveness of such outbound protection relies on customers implementing its elements, which mostly benefit recipients of the organization's email. On the inbound side, Google asks administrators to set up a Domain-based Message Authentication, Reporting & Conformance (DMARC) record to check either the SPF record or the DKIM signature on the incoming mail. If either passes, the email is usually let through.

Gmail does throw up warning banners when even this low bar fails, but only for its own apps and Web pages.

And that's pretty much it for Gmail's anti-phishing technology.

INKY Email Security

Layering INKY on top of Gmail catches a lot more phish. Rote methods like DMARC analysis of SPF or DKIM don't protect against account-takeover and domain-spoofing attacks. An account takeover involves a bad guy repurposing a legitimate account to his own evil ends.

A spoofed domain — one that looks like Google but actually has an upper-case "I" instead of a lower-case "l" — may appear benign to the casual observer, but actually come from a server that distributes poison. The domain may be "legitimate," according to DKIM, but may not belong to Google.

Attackers may use imagery to further confuse the recipient. A logo may look like Citibank's, but the email comes from somewhere else entirely. The sender is relying on the recipient not observing too closely.

INKY, a virtual appliance that sits in front of an email server, analyzes an email multiple ways. In addition to looking at the entire record the way a machine does, it also uses computer vision to "see" the mail the way a human would. Thus, imagery indicating that an email seems to be from Citibank (e.g., it has the bank's logo, font, and color) is compared to what the machine sees, which is that the email actually originates from a server in Malaysia registered to an automobile parts distributor. Artificial intelligence and machine learning allow INKY to detect that Citibank spoof, even if the logo's dimensions are slightly distorted or the color is off, which are some of the ways the black hats try to get around visual analysis.

After analysis, INKY inserts a banner at the top of every email: red for known or highly suspected bad sender, yellow for spammy looking material, and gray for mail from a safe domain or sender.

INKY is fully integrated into Gmail, installing in 30 minutes or less. Self-adapting to new and evolving threats, INKY requires no coding or configuration beyond initial setup, integrating quickly to any environment. As emails are received, INKY starts comparing models and building profiles to manage and anticipate the bewildering complexity of email attacks. The more it learns, the more it sees.

Things INKY doesn't do:

- Prevent email from being delivered
- Impede day-to-day functionality

Things INKY does:

- Act as an invisible sentinel ensuring fidelity without compromising content

INKY is fast. In about two seconds, INKY processes an email and transfers it back to the Gmail server for final forwarding to their recipients inbox.

INKY and the Inbox

In addition to affixing banners, INKY also alerts users when they attempt to click a link or respond to the email, presenting them with a more direct warning and an analysis of the likely outcome if they choose to proceed. INKY provides active, targeted guidance in every email. Warnings are simple, yet direct, and are delivered across desktop and mobile platforms for a harmonized user experience.