SOLUTION BRIEF

INKY™
A Kaseya COMPANY

INKY vs. Microsoft Email Security

Understanding how INKY protects organizations from phishing attacks better than Microsoft's built-in security.

Microsoft offers some protection from spam, malware and phishing attacks through the Exchange Online Protection (EOP) and Exchange Advanced Threat Protection (ATP) packages. While these packages attempt to stem the rising tide of Business Email Compromise (BEC) attacks, they aren't entirely succeeding.

Spam and malware capabilities are mostly the same between Microsoft EOP/ATP and the INKY solution and are in line with the rest of the cyber industry: both solutions identify known and zero-day spam and malware. Where EOP/ATP and INKY differ is in the approach to phishing.

EOP/ATP solutions rely on threat feeds to identify phishing emails: these are real-time streams of known bad URLs. When EOP/ATP detects a reported URL in an email or attachment, it knows the email is a phishing email. Unfortunately, many phishing campaigns still get through EOP/ATP, because the attacker's emails either do not have URLs or have randomized URLs, where every recipient gets a different URL.

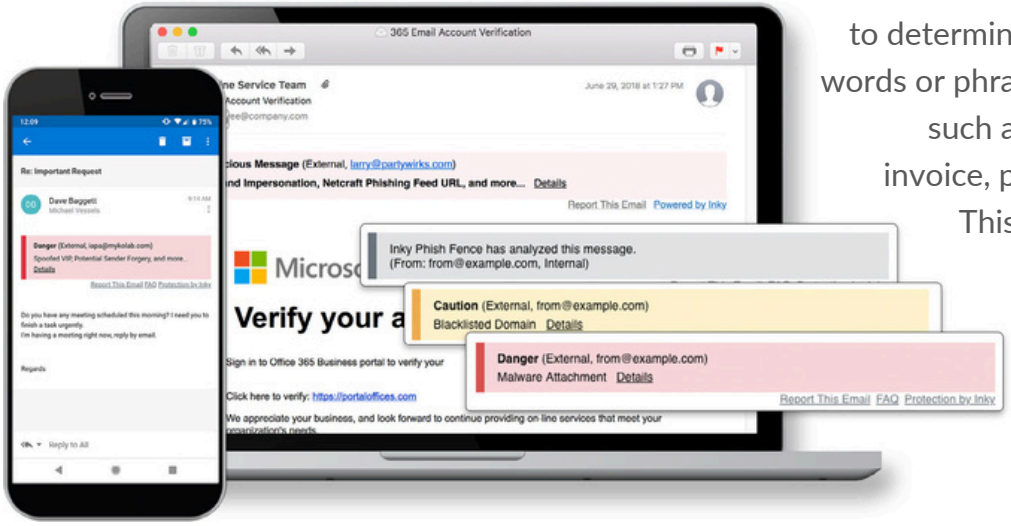
Thus, one victim reporting the URL to the threat feed does not help another victim, because the second victim's phishing URL is different. This document describes specific kinds of threats, the limits of the Microsoft EOP/ATP solution on dealing with each threat type, and how INKY can stop these next-generation phishing attacks.

Dangerous content

Both Microsoft and INKY rewrite dangerous links so that if the user clicks a bad link, the user is taken to a holding or "proxy" page. The key difference is that while Microsoft EOP/ATP looks up the URL in its threat feeds, INKY goes a step beyond to render the page and examine the HTML page content for signs of phishing, malware, and credential harvesting.

So even if a page has never been reported to any threat feed, INKY can determine — by directly analyzing the page content in real time — that the page is malicious.

INKY also analyzes text within each email and attachment to determine if sensitive words or phrases are used such as: password, invoice, payment, etc. This will then be flagged in the warning banner.



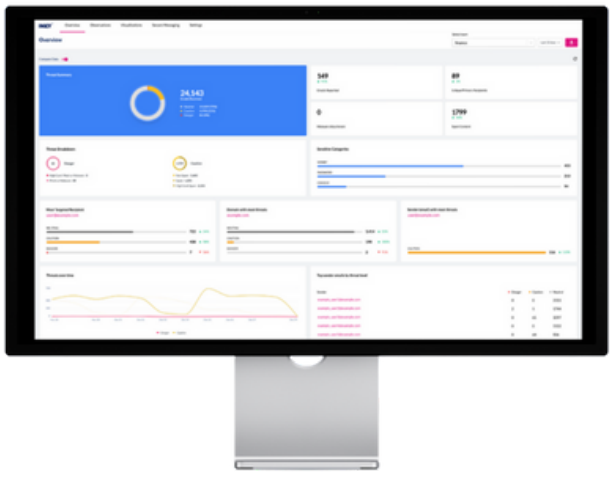
SOLUTION BRIEF

The banners

INKY's email protection software places user-friendly warning banner and reporting links directly into the email. Microsoft does not offer any type of warning banner. The banner is visible on both desktop and mobile email clients. No matter what type of device, INKY supports it. The banners offer specific guidance to both protect and educate users giving them important cues about the contents of an email and allowing them to take a closer look or proceed cautiously. INKY's ability to work on mobile devices is unique technology that no other anti-phishing solution offers. Customers can also use these banners to provide policy guidance to end-users.

Spear phishing

Microsoft relies on simple address matching to determine if a sender is impersonating an individual. Specific policies can be created for individuals such as executives, but these policies ony catch the most obvious spear phishing attempts. INKY offers behavior profiling through artificial intelligence (AI). INKY employs true machine learning to build a data rich social graph of senders and sender profiles. Should some piece of a communication not align with the profile, the system attaches a warning for a potential impersonation then learns from your feedback.



Brand forgery

Again, Microsoft ATP depends on address (or similar looking address) matching, so that an email from user@ docxsign.com will be flagged as suspicious because the sender's domain is similar to a well-known, commonly- forged sender domain. The problem with this limited approach is that there are innumerable domains that attackers can create that look plausible to recipients. For example, a recent phishing campaign impersonating American Express used domains following the template aexp-<xx>.com. These domains are believable to recipient victims but dissimilar enough to real American Express sending domains to completely fool EOP/ATP.

The INKY solution is computer vision that scans the email for visual brand indications:
by seeing each like a human does, INKY identifies logos and logo-like text to identify the brand as human eyes would. Further, INKY detects nearly imperceptible font and character anomalies that busy employees overlook.

Deep sea phishing and zero-day attacks

ATP cannot block these cleverly constructed campaigns that are designed to bypass email filtering products. Traditional systems rely on records of previously identified attacks, which does nothing to stop the deluge of new attacks launched every day. INKY employs computer vision, AI, and machine learning to identify even zero-day phishing attacks.