IT (Information Technology) managers already paying hefty fees to email providers, security companies, and spam filtering firms are not looking to layer yet another bill on top of all that. But phishing protection is the most judicious investment they could make. Going without it is risky businesses.

The truth is that the best-looking phish are the most dangerous. That innocent email from Microsoft about a software update is a perfect copy of the HTML from a real Microsoft notice...with just one invisible link changed. When missed, it's the one oversight that leads to a credential-harvesting or malware-injection site.

Most email security solutions use models, based on previous experience, of what a good or bad email looks like. An email that looks bad compared to the model is flagged. The good-looking ones are let through. But the problem with this is obvious: the best-crafted phish slip right through these systems.

For short money, INKY protects against this type of attack. It's not that INKY doesn't also use reference lists of known bad sites or build models for sender profiles. It does all that as well. But most importantly, INKY protects against zero-day exploits in a way that other solutions can't.

Here's how it works. INKY sits in line between the secure email gateway and the client device. (computer, phone, or any other email platform) From that vantage point, INKY looks at every email two ways: as a human would and as a machine would.

The human part goes as follows: When an email passes to the INKY software-as-a-service (SaaS) module, one branch of the analysis renders the email's HTML code to produce an image, which is what the recipient would see. Using computer vision techniques on this image and internal references — like the top 250 most-phished brands and a VIP list of the recipient's company's top executives — the analysis decides what the email is purporting to be. Does this look like it's coming from Microsoft? From Dropbox? From DocuSign? From the president of the company? From the chief financial officer?

While “holding that thought,” INKY turns to the machine part of the analysis, seeing not just what we humans see, but also taking a thorough look under the hood. That's where INKY's machine side not only finds all the text that ends up in the humanly readable email, but lots of other interesting information as well. In the header, most of which is not rendered for human consumption, lies the often-confusing path that the email took to get from sender to recipient. The analysis finds the original sender.

Comparing where the email "appears" to be coming from with where it actually came from, INKY can see when there's a problem. This note was supposed to be from Microsoft, but actually came from a parts factory in Istanbul. INKY throws a flag.

The shop in Istanbul may be legit. The email's DKIM signature indicates that it hasn't been tampered with since it left the shop. Its SPF record indicates that its IP address is indeed a legal one, legitimately able to send email. Maybe the owner's daughter's boyfriend got the account credentials and sold them to a black hat. Except INKY doesn't care about the maybes, and it certainly doesn't certify an email as safe just because some of its parts look legitimate. It sees that the Turkish factory ≠ Microsoft and throws a flag.

Now, most of the incumbent secure email gateway (SEG) providers — Microsoft, Google, Proofpoint,
INKY is a cloud-based email security solution. It blocks spam, malware, and — most importantly — phishing attacks. INKY uses unique computer vision, artificial intelligence, and machine learning to catch pretty much everything. She’s driven, curious, mobile, and she’s growing smarter by the subject line.

Schedule a demo today.

www.inky.com