INKY™

Rolling the Dice:

Risking a 1 in 10 Chance of a Catastrophic Phishing Event

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, Mimecast — incorporate some sort of phishing detection into their platforms. However, INKY sees the output of these platforms because it sits downstream, and they're clearly not doing enough. It's true that phishing attempts represent a small portion of all incoming emails; usually less than 1%. By the INKY team's metrics, the incumbent SEGs typically block around 90% of this 1%. Which means only 0.1% get through. Statistics to brag about, right? Wrong!

It's that 0.1% of phishing emails that have the most dangerous payloads. And, in an environment that gets 100,000 emails per day, the incumbent SEG systems will pass 100 phishing emails straight through to recipients every day. Those 100 emails got through because they were sent by the most sophisticated threat actors — exactly the ones likely to do the most damage to the company.

Metaphorically, it's like a missile defense system that blocks 900 incoming nuclear warheads a day but allows 100 through.

So, it's clear, 90% isn't enough.

An example or two shows why it's worth a bit of phishing insurance to protect against the ever-cleverer phishers:

- A skillful hacker set up email accounts and a Latvian shell company to pose as Taiwan-based Quanta Computer. He made phishing emails that looked like Quanta Computer invoices. He impersonated real employees, used real-looking contracts, and targeted known purchasing staff. He scammed Google out of $23,000,000 and took Facebook for $98,000,000. Wouldn't you pay a few bucks a month per seat to protect against that?
- Impersonating the CEO of Crelan Bank, a single phishing email to an employee in the finance department led to a €70,000,000 wire transfer, which the company discovered only during an audit.

Damage from the twelve costliest phishing attacks that became public (most don't) totaled nearly $500,000,000. Surely, investing in phishing protection would have been the better choice.

A couple of final points. To those who worry about INKY "reading" their email, the modules do read the email for analysis, but no humans do. When a user reports a suspected phishing email through the INKY reporting tool, the INKY team will read the mail, but not under any other circumstances.

Who or what reads email is important because when a machine analyses the mail, it won't see the term "Office 365" written backwards (563 eciffo). When the recipient sees it, it will look right because the renderer will act on the "bidirectional text" indicator (often used for Arabic or Hebrew) and will play the characters backward, making them appear as "Office 365" to the human eye. All the machines will miss this ruse because it's designed to evade them, but INKY has the human part of the analysis to use for comparison. INKY will find that, while this email seems to be about a Microsoft product, it actually came from a factory in Istanbul — and therefore conclude that it's a phish.

This is the sort of protection you want. The risks of being victimized by a phishing attack are ever-present and non-negligible. For example, 30% of phishing emails are opened by the recipient. And the average cost of a phishing attack for mid-size businesses is $1.6 million.[1] When the probability and cost of a potential phishing event is weighed against a relatively small investment in anti-phishing measures, the value of that investment is obvious. Going even a day without the protection of INKY is a gamble you probably don't want to take.

[1] Source: https://blog.dashlane.com/phishing-statistics/

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

INKY®