INKY®

UNDERSTANDING PHISHING

How a Ransomware Attack Unfolds

Since virtually everyone saw the Colonial Pipeline attack in the news media, ransomware has become a household word. Most people understand that ransomware involves black hats putting code on people's computers that, once triggered, causes them to lock up, and some people even know that encryption is involved, but few are aware of the step-by-step details. In this Understanding Phishing guide, we lay out the methods used by ransomware attackers and make the connection between ransomware and phishing.

Overview

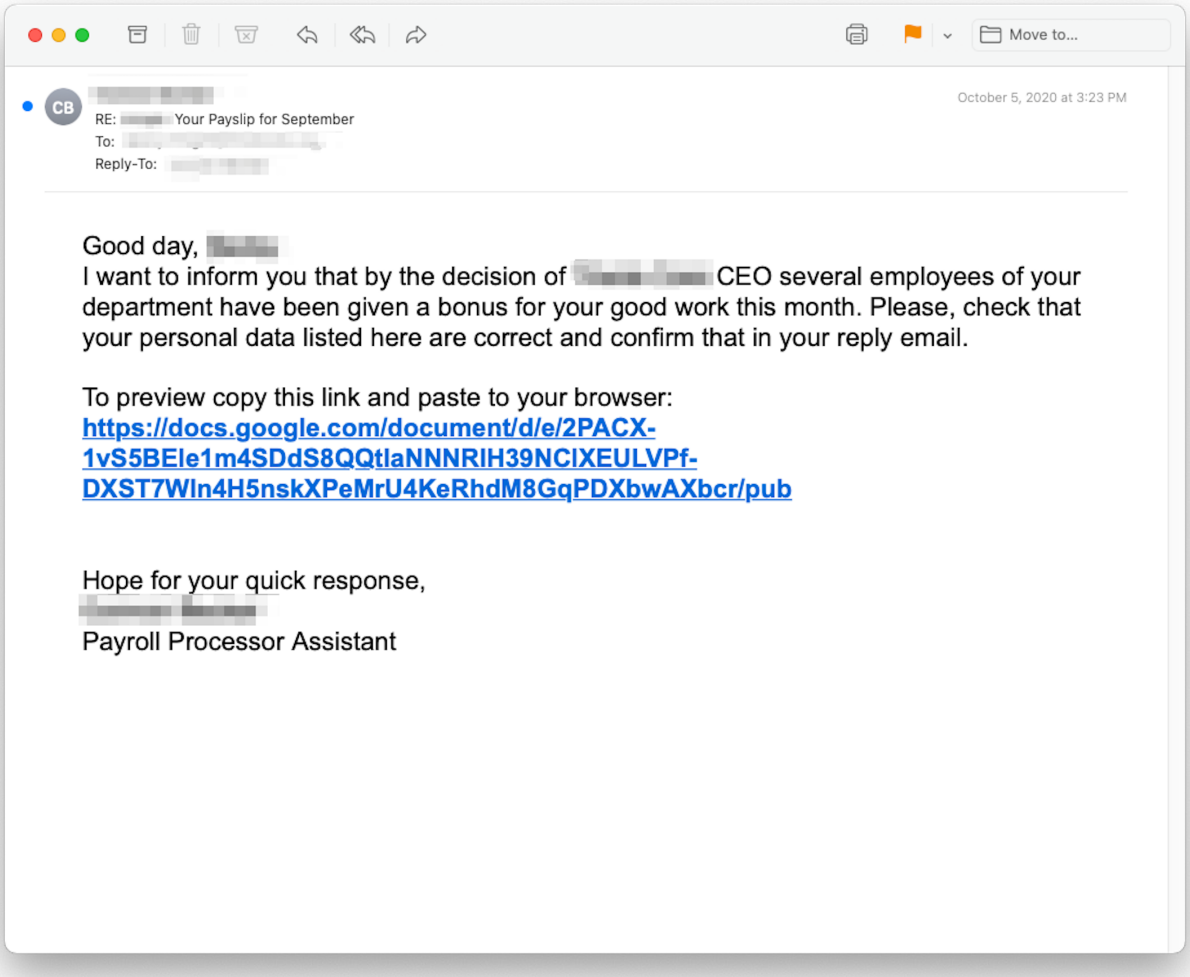
Recent ransomware shutdowns of infrastructure companies such as natural gas distributor Colonial Pipeline, meatpacker JBS USA, and British healthcare provider Health Service Executive have greatly raised the visibility of this type of attack. And yet, most people do not understand the connection between ransomware and phishing.

The simple explanation is that most ransomware shutdowns start with a successful phishing attack. There were 2,464 ransomware incidents in 2020, according to the Federal Bureau of Investigation, and 91% of cyberattacks began with a “spear phishing” email, according to TrendMicro. Within the category of cyberattacks, ransomware deployments were kicked off in 67% of cases with a phishing email, according to PurpleSec, which also noted that ransomware cost victims $20 billion in 2020.

The average payment organizations made to escape ransomware perpetrators’ clutches rose to $312,493 in 2020, up 171% from $115,123 in 2019, according to University of California, San Francisco. Prominent victims include CNA Financial ($40 million), the aforementioned JBS ($11 million), Brenntag (4.4 million), and Travelex (2.3 million).

Not the Payroll Processor's Assistant

In this closeup view of a recent example, the attackers sent phishing emails impersonating the Human Resources department. These emails were assembled using dynamic algorithms to parse out local-part (whatever occurs before the "@" in an address) and domain info, thus personalizing the mails for each recipient.



Lures used in this campaign included annual bonus notifications, customer complaints, employee surveys, employee termination notices, priority task lists,

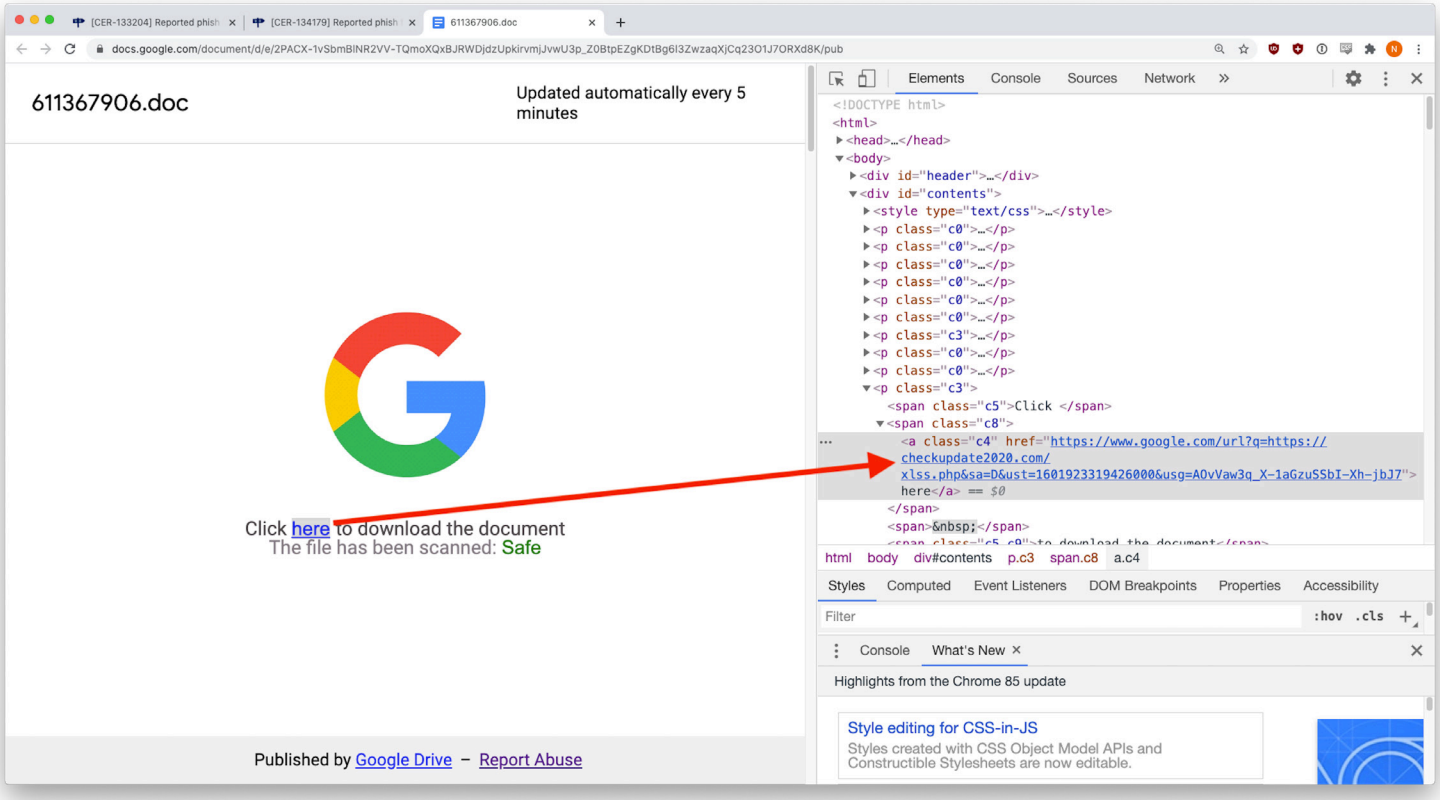
INKY™

and outstanding bills.

The emails themselves originated from hijacked legitimate accounts, which were able to pass authentication checks. In some cases, they were spoofed to look like they came from a real vendor's domain.

The malicious emails were able to bypass the secure email gateways (SEGs) because the only link in the messages was to a legitimate cloud-based resource (e.g., GoogleDocs, ZohoDocs), which was co-opted to host a link that, on a click, injected malware into the victim's system.

Taking a closer look at the cloud component, INKY engineers found that the attackers abused GoogleDrive to create a customized document template, which sported Google's logo and the false statement "The file has been scanned: Safe."



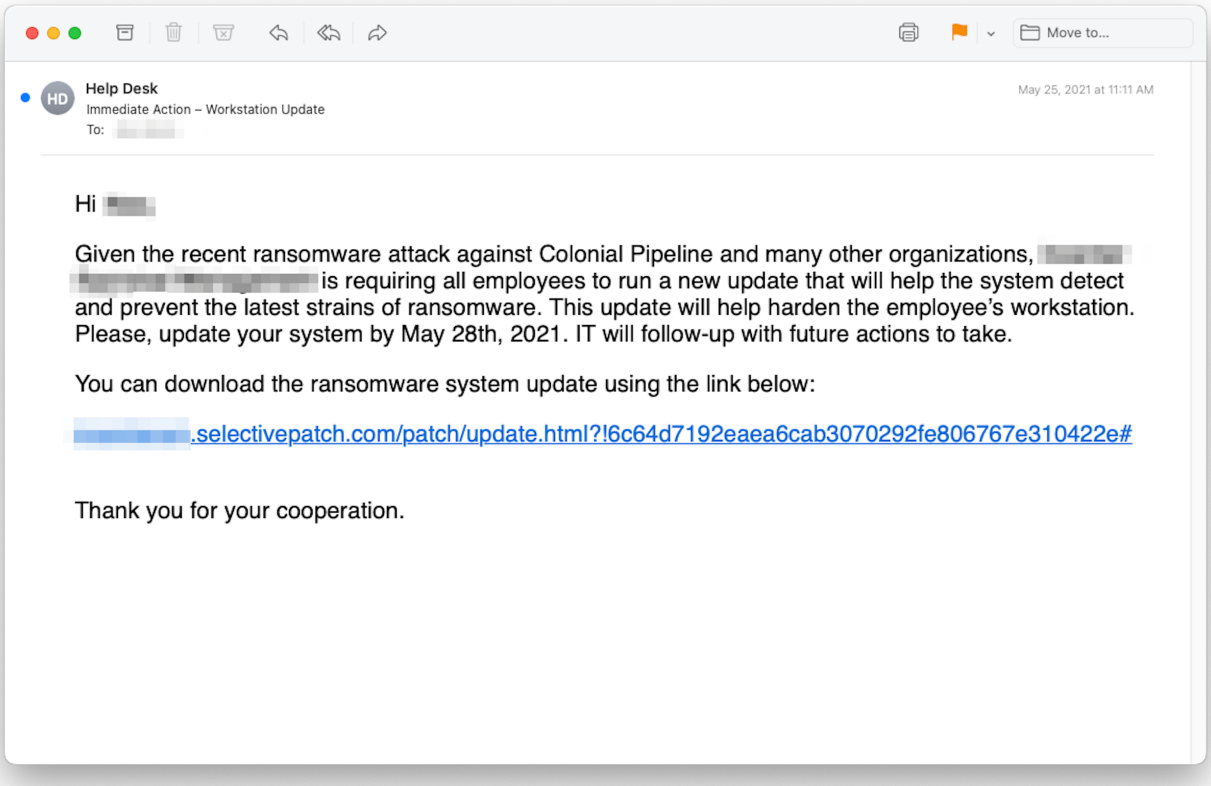
In that bogus customized document, the black hats placed an automatic malware download link, which was able to evade Google's detection by using **`google.com`** as an open redirect to **`checkupdate2020[.]com.`** Google is one of many sites that allow open redirect, which involves placing a link within a link that misleadingly takes a victim to an unexpected website.

The attackers' goal was to disseminate TrickBot and BazarLoader malware, which would deploy and open a back door on the victim's system, allowing a command and control (C2) server to infect the system with Ryuk ransomware, which would encrypt all files using AES-256 encryption.

A sophisticated method, Ryuk identifies and encrypts network files and disables Windows System Restore to prevent victims from recovering their files, unless they have an external backup.

Colonial Pipeline Kicks Off Opportunistic Attacks

In this ransomware attempt — caught by INKY — the bad guys took advantage of the successful phishing-led ransomware attack executed against Colonial Pipeline to try to scare their targets into downloading malware. By posing as an internal sender (Help Desk), the attackers purported to being doing the opposite: requesting users to download an "update" that would protect against malware.



Help Desk
Immediate Action – Workstation Update
To:
May 25, 2021 at 11:11 AM

Hi

Given the recent ransomware attack against Colonial Pipeline and many other organizations, is requiring all employees to run a new update that will help the system detect and prevent the latest strains of ransomware. This update will help harden the employee's workstation. Please, update your system by May 28th, 2021. IT will follow-up with future actions to take.

You can download the ransomware system update using the link below:

.selectivepatch.com/patch/update.html?l6c64d7192eaea6cab3070292fe806767e310422e#

Thank you for your cooperation.

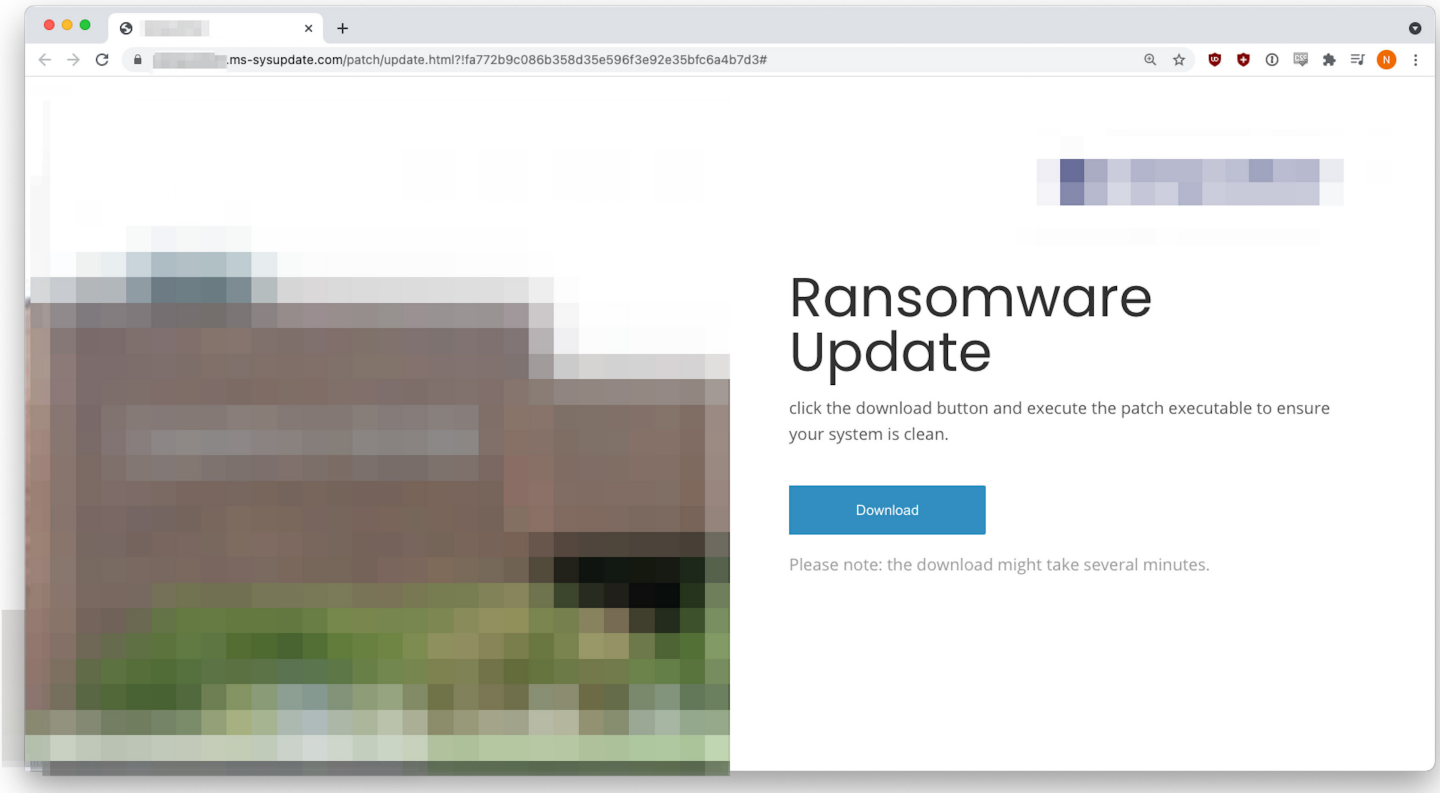
The black hats bought domains — **selectivepatch[.]com** and **ms-sysupdate[.]com** — from NameCheap in late May (the **ms-sysupdate.com** WHOIS record is shown below). As the dates make clear, they immediately began sending phishing emails from those domains to targeted recipients.

```
Domain Name: MS-SYSUPDATE.COM
Registry Domain ID: 2613602127_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-05-20T15:31:19Z
Creation Date: 2021-05-20T15:03:35Z
Registry Expiry Date: 2022-05-20T15:03:35Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
```

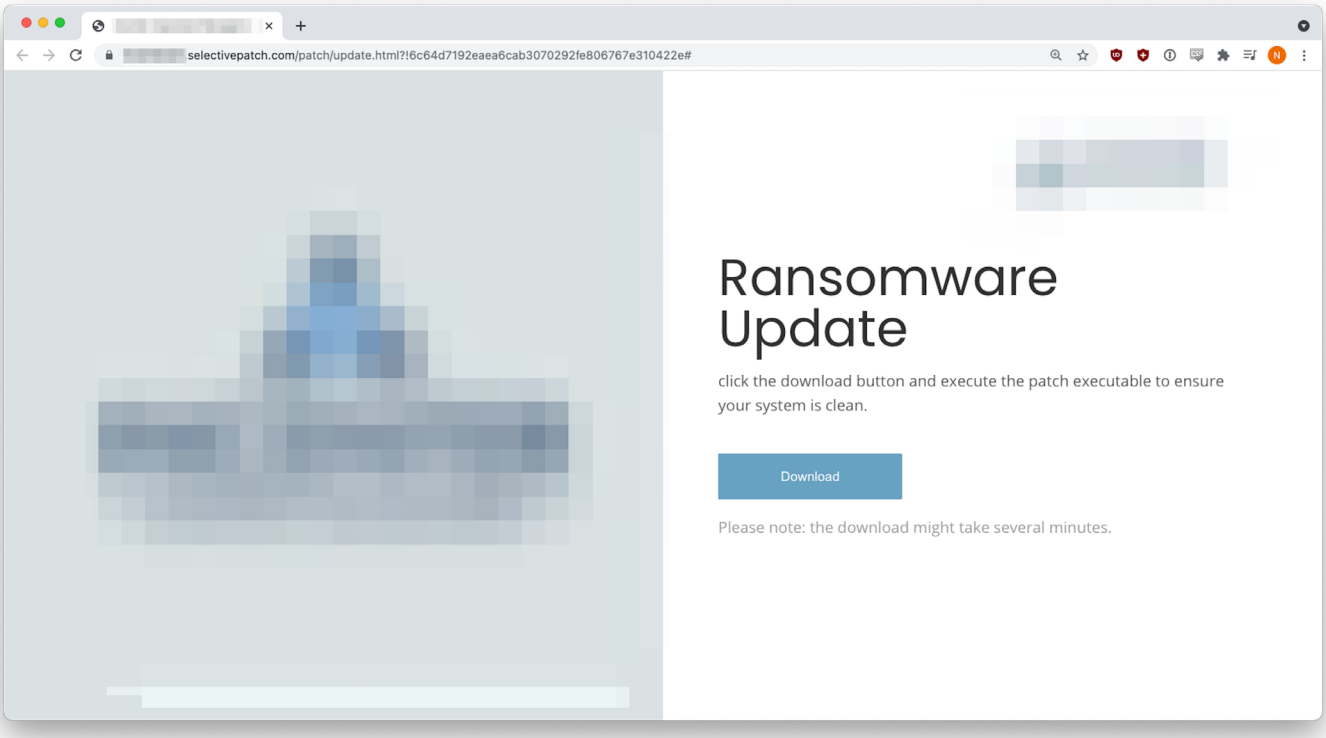
NameCheap has, shall we say, “liberal” customer policies, for example, allowing all manner of registrations and accepting cryptocurrency as payment for domains and cloud hosting services. Given that ease of doing business, the attackers used the same domains to both send the phishing emails and host the malware. How convenient!

In a nice touch, the bad guys used the target company’s name as a subdomain in the malicious link to make it look like the email was an internal request.

Here’s the slick malware injection site hosted on **`ms-sysupdate.com`**:



And the one hosted on **`selectivepatch.com`**:



Note that in both cases, not only was the target company's name used as a subdomain, but its logo and brand imagery were also sprinkled around liberally on the landing page.

The big blue Download button initiated a download of a file called "**`Ransomware_Update.exe`**".

Payload: Cobalt Strike

Rather than protecting against malware, however, the payload was itself malware, in fact a particularly pernicious variety called Cobalt Strike. Although Cobalt Strike started out as a legitimate tool used for penetration testing, its source code was leaked in 2020. Since then, it has been ferociously abused by phishers.

Common anti-virus (AV) systems, which focus on security data, often miss Cobalt Strike, which implements two main techniques to avoid AV detection: it obfuscates its own shellcode and leverages a domain-specific language called Malleable Command and Control (Malleable C2).

To detect executables, AV systems commonly implement sandboxing, which provides a separate environment to run and inspect suspicious executables. Cobalt Strike, however, hides shellcode over a named pipe. If the sandbox doesn't emulate named pipes, it will not find the malicious shellcode. In addition, the attacker can modify and build their own techniques with the Cobalt Strike Artifact Kit.

After establishing itself in a system, Cobalt Strike can mimic popular services (e.g., Gmail, Bing, Pandora) to evade detection. The platform uses Malleable C2, which lets attackers modify Cobalt Strike command-and-control (C2) traffic at will. The attacker can then identify legitimate applications within the target organization, such as Amazon traffic, and modify the C2 traffic to appear as Amazon traffic using any number of publicly available profiles.

Cobalt Strike is highly customizable and can be used for command execution, key logging, file transfer, SOCKS proxying (to get around firewalls), privilege escalation, port scanning, and lateral movement.

INKY Prevents Phishing that Leads to Ransomware Shutdowns

As the reader will note, INKY caught the phish in the preceding examples. To prevent ransomware, organizations need to stop the attack at the beachhead. All it takes is one successful phishing exploit, and the network falls to the mercy of the attacker.

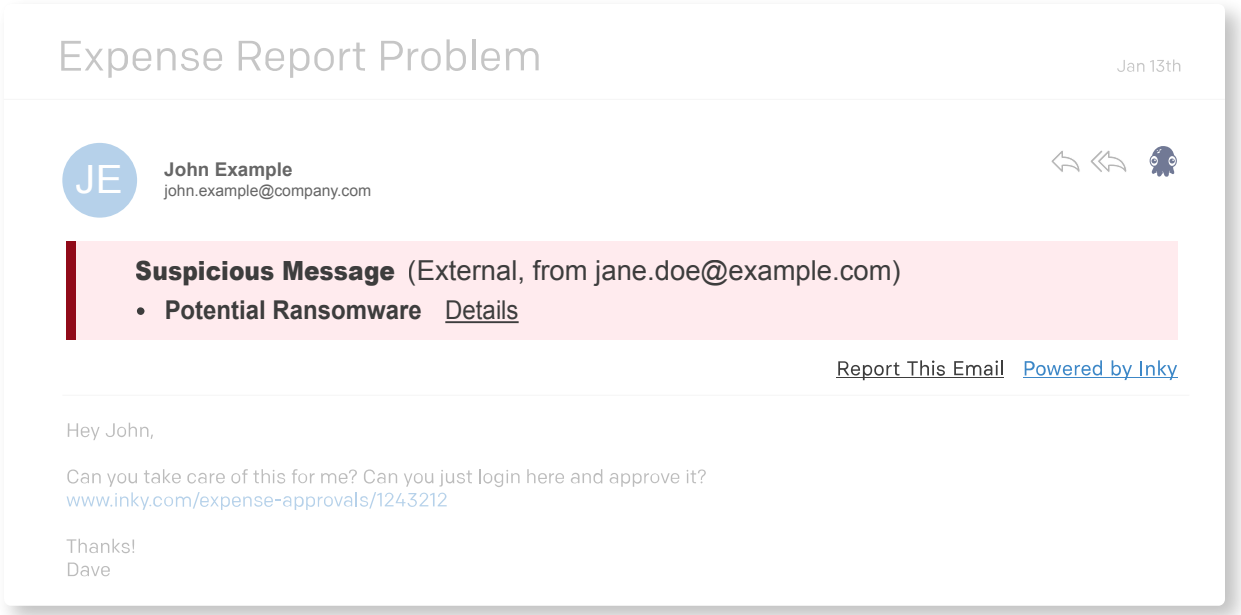
INKY is the most advanced phishing software on the market.

INKY™

How does INKY work?

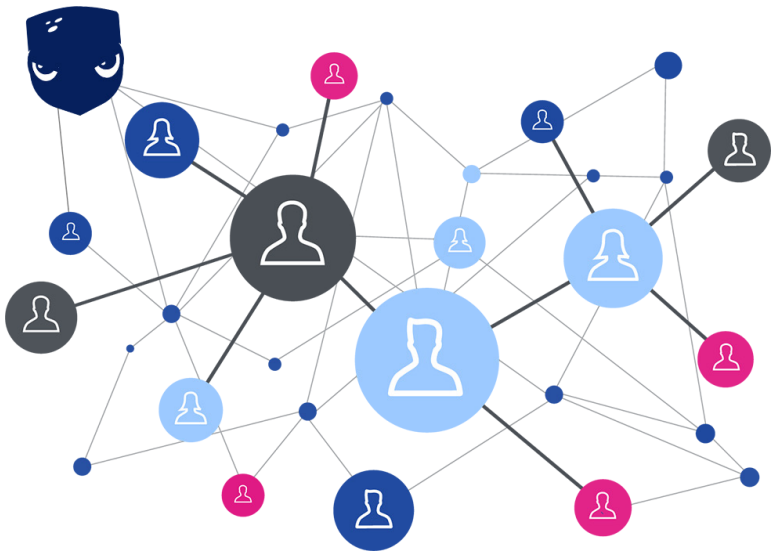
INKY unleashes its swarm of mathematical and behavioral models on every email that leaves the secure email gateway (SEG) on its way to recipients' inboxes. These models all operate in parallel, completing their full analysis in less than two seconds and giving each message a grade. The result is communicated to the recipient by an inserted HTML banner — colored-coded gray (safe), yellow (caution), or red (dangerous).

When an email hits a tripwire in any of the dozens of models in INKY's arsenal, that result is surfaced to the banner. The recipient sees why INKY threw a flag, training them while keeping them safe (e.g., INKY sandboxes all live links, among other measures). Key models perform first-principles analysis while others make database references. Visual analysis is performed in a headless browser, and detected brand elements (e.g., logos) are compared to the real domain of the sender, which is determined by analyzing the header information.



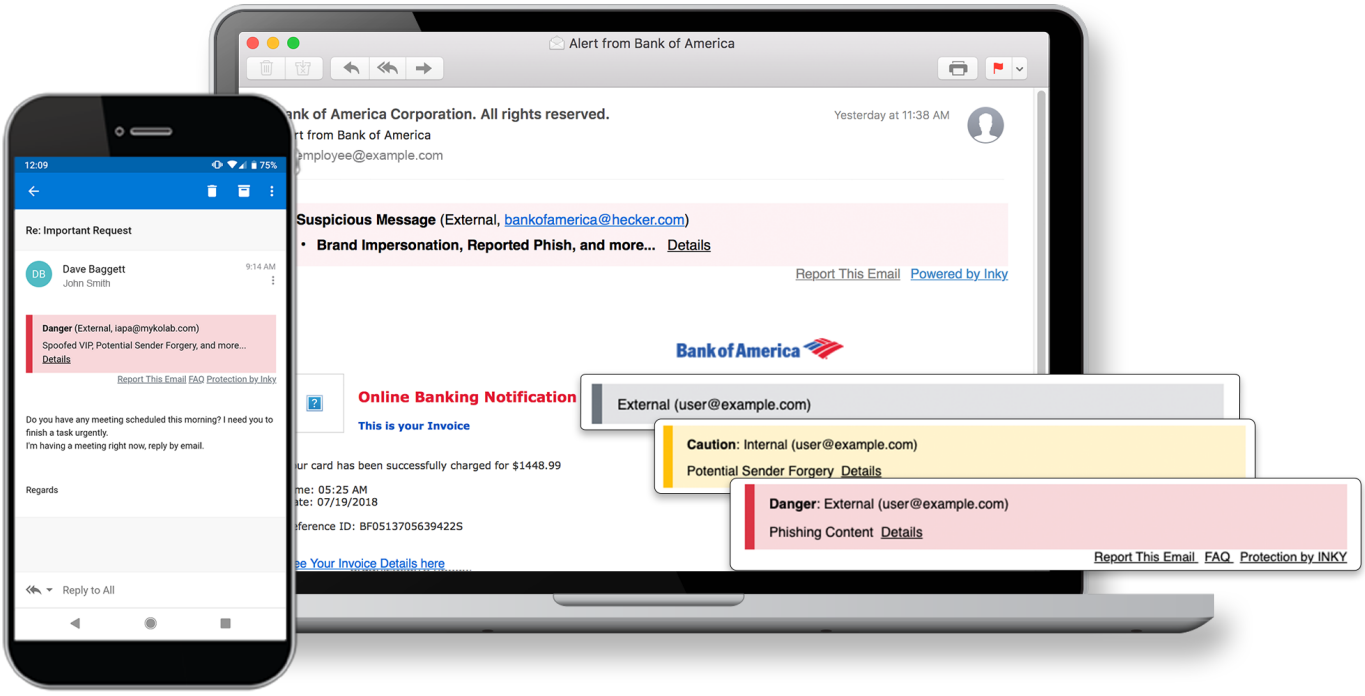
INKY™

INKY has learning models as well. Immediately after installation, INKY begins to track who sends an email to whom, establishing a social graph of sender profiles within a week or so. These profiles accumulate not just senders' identities but their detailed attributes as well. For each recipient, INKY stores a stylometry profile of their senders. This profile could contain their usual signoff, types of punctuation typically used, primary location, email platform, or device type. Then, INKY undertakes cluster analysis to decide if the set of attributes of any incoming email fits with the known sender profile. If the style is too far out of line, INKY warns of an impersonation.



For example, If the chief financial officer never uses ellipses when he's sending email to you, and one day an ellipse-festooned email comes in, looking on a smartphone like it's from him, INKY notices the difference and flags it with a Potential VIP Impersonation in the banner.

With its wide array of complementary analyses, INKY catches even the faintest whiff of phish. And catching all the phish is the best way to protect against ransomware. If the black hats never get a toehold, they can't put malicious code on the target machine, its neighbors, and ultimately the entire organizational network.



Request a demo.

We're passionate about email.

Ready to talk about an issue you're facing with email security at your organization?

www.inky.com