How to protect your emails using Inky Phish Fence: Why phishing is your biggest current threat

A white paper for Inky Technology Corp.

By David Strom
http://strom.com
@dstrom

November 2017

David Strom is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 30 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom's Hardware.com, and the editor of Inside Security's regular email newsletter. He began his career working in varying roles in end user computing in the IT industry.

Introduction

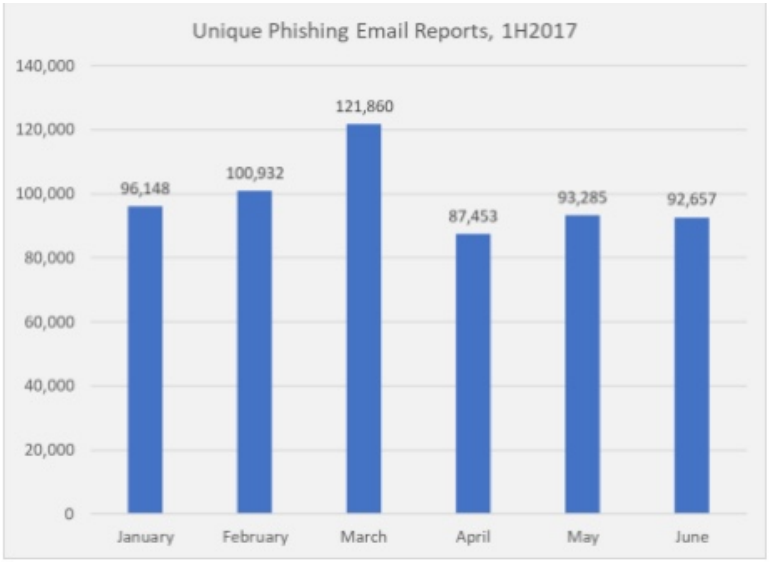
The Office 365 email inbox (and for that matter, other inboxes too) has become ground zero for the next corporate malware infection. This is because email phishing attacks have become the gateway drug for exploiting your enterprise. Whether it is ransomware, data leakage, or targeting your CEO or CFO, a single email that is mistakenly clicked on can lead to all sorts of trouble – and expense -- down the road.

The latest study sponsored by Google finds that victims of phishing are 400 times more likely to have their account hijacked than a random Google user. **Automated phishing construction kits** enable a higher rate of account hijacking because they capture the same details that Google uses in its risk assessment when users' login, such as victim's geolocation, secret questions, phone numbers, and device identifiers.

As if that wasn't enough, take another recent example of how several high-level staffers at the White House were recently fooled by an email prankster into thinking they were responding to legitimate messages. While not exactly malicious -- the sender was merely making a political point, rather than trying to infect anybody's computer, it shows how even someone who is in charge of setting cyber policies for Homeland Security can be easily fooled. And while we are talking about government email misuses, consider this recent analysis by Proofpoint of millions of email messages that they tracked in October. During that month, a tenth of these emails didn't even originate from US IP addresses! And one in eight messages was found to be fraudulent.

A report last December from PhishMe found that 91% of cyberattacks start with a phish. The study took place from January 2015 through July 2016 and studied millions of emails. An FBI report from March 2017 found that business email compromise scams, many of which have included phishing attacks, have resulted in $5.3 billion in financial losses since October 2013.

Phishing is certainly on the rise. The 2016 report from the independent Anti-Phishing Working Group in February stated that there were more than a million attacks last year, which was a 65% increase over 2015. The numbers of unique campaigns has risen to about 90,000 per month since last year, and has remained steady throughout the first half of 2017.



Attackers have also honed their skill with all sorts of disguises. They are counting on the fact that most of us aren't paying attention when we are scrolling through our messages. Since many of us use our phones for taking the first pass at our messages, attackers are counting on the fact that we are often distracted or not as careful at examining the structure and composition of the messages, not to mention that the smaller screen sizes make it harder to really carefully examine a message and figure out if it is legit or is sent by a criminal.

But even if you are reading your inbox on the biggest of desktop screens, there are all sorts of non-technical cues that attackers put in their phished messages. The reasons why Locky's phishing campaign was effective had to do with the way the messages were crafted, including presenting them in a business context with a personalized message to the recipient. This story on *Dark Reading* also mentions that there were no noticeable errors in grammar or spelling and the message deliberately mimicked many organizations' existing invoice processes.

And **all it takes is just one message to slip by,** and an attacker can be inside your network, connecting to your endpoint and trying to leverage that access to plant additional malware, take control over critical servers, and find something that can be used to harm or extort funds.

Common exploits

Let's look a few common phishing exploits, and how the technology behind them is improving and evolving.

The early days of phishing seem so quaint now. Back then, a phished email used very simple tricks: a hyperlink that took a reader to a different URL than was specified in the text of the link, or a **typosquatted domain** that was different by a single character or a transposed pair of characters, like Netfilx.com instead of Netflix.com. Another approach is to substitute the number 0 for the letter O in domain names. If you weren't reading carefully, you wouldn't think anything of just clicking on that innocent link.

Phishers make their attacks less obvious by registering their squatted or similar domains, and taking things a step further. They copy the "real" site's images, fonts and page layout and design so you won't notice their trickery at a glance. Then try to get you to login using their scammy page, where they capture your credentials and then steal your account and possibly your money too.

Then came more targeted phishing, what is called **whaling** because it aims to send a message to impersonate the "big fish" executives such as the CEO or CFO. A message would appear to come from this person, but in reality is just a spoofed address or an address that contains some portion of the executive's name. Typically, a whaling attack is looking for money, such as asking the victim to transfer funds from the corporate bank account to the criminal's account.

Another targeted attack is called **spear phishing**, because a criminal is going after a very specific person, organization, or position within a company. The attacker includes the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender. Again, spear phishers are looking for confidential data that they can use to exploit or sell on the black market. A recent example of this attack was the FreeMilk campaign that customized emails with decoy documents for each intended recipient.

Credential harvesting is another specialized attack form. Attackers try to get users to login to fake Google Docs or Dropbox or other cloud-based accounts in the attempt to steal their credentials. Criminals craft web portal pages that mimic the real thing, and then send emails with links to them in the hopes that a victim will fill them out and provide their username and password which are then captured and used for further exploits.

Pharming or DNS poisoning is yet another phishing method, where traffic is redirected by using exploits or tricks in the DNS protocols so a user thinks he is browsing the intended site but is actually on the criminal's website. It is often used to get credentials, or to obtain information to appropriate someone's identity.

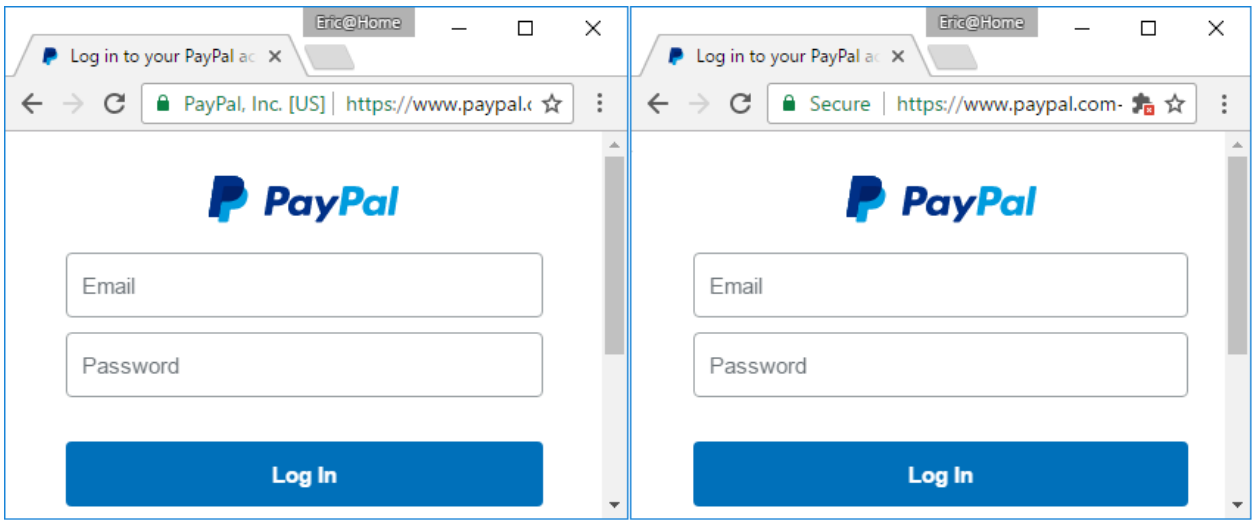
Another method is **smishing**, which is a combination of social engineering techniques that are sent over SMS texts rather than using the typical emails. Criminals try to get you to believe that they are a trusted correspondent and then give them your account information. In one recent case, a criminal gets you to use your bank's step-up authentication to send you a real text authentication query, which the phisher then uses to compromise your account. Certainly, the attackers are getting more clever.

The latest round of attacks takes the typosquatting technique a step further. Even if you are the sharpest-eyed observer, you will have a hard time detecting this technique that goes by the name punycode or **homographic typosquatting attack**. The idea is simple: back in the day, the Internet standards bodies expanded the ability to handle non-Roman alphabet characters for domains and URLs. The trouble is that many of these characters look very similar to the ordinary ones that you and I use in our Roman alphabet. Spammers purchased domains that looked just like the all-Roman letters, with one or two changes using some other character set. For example, if the domain "apple.com" would be registered as "xn--80ak6aa92e.com" it would bypass these filter by only using Cyrillic characters.

This post from **Wordfence shows how subtle these homographs really are**, making it almost impossible for anyone to detect. There is further discussion on this site about how these kinds of phishers operate.

A new kind of attack is to leverage one of the Tor anonymous browsing services called SMS Privacy and use it to launch phishing campagings.

Finally, there is another series of attacks that combines one of these methods above with **using phony SSL certificates**. Sadly, it doesn't have a adorable pun-like name unlike the other attacks. Having a faked cert means that it is harder for victims to distinguish the phished site, because it carries the green lock icon that indicates the site is using SSL. Can you really tell the difference between these two images below as to which one is real and which is the phished message?



One real, one fake, your account is at stake.

Ironically, an effort that began several years by Google and the non-profit foundation behind the Let's Encrypt website have made problems worse with trying to distinguish proper certs. Let's Encrypt makes it dirt simple to obtain a free SSL certificate in a matter of seconds, so that showing warning signs in the URL bar of browsers when you aren't connecting to a secure website are almost moot now. While it is great that the increasing majority of all web traffic is now encrypted, we need better mechanisms that just a red/green indicator to help users understand what they are viewing.

Zscaler researchers have seen 12,000 daily phishing attempts delivered over SSL in the first half of 2017, a 400% increase from 2016. Eric Law's post here discusses more of the issues involving SSL certs. While these issues aren't new (check out this decade-old paper on the issue), it is getting worse. Even more extensive research into certs can be found from Troy Hunt here.

Defensive maneuvers

So the first line of defense is often figuring out one or more of these phishing techniques, and then trying to stop them. Over the years there have been a number of efforts to increase defensive mechanisms, including better browsers, more thorough phishing training, and better email filtering. All have seen mixed results.

Until recently, **browsers still had pretty miserable defensive mechanisms**. When ZDnet last did a comparative review back in 2013, the best browser was Opera which still let through more than 5% of the scam emails, and the worst was Mozilla Firefox, which allowed 45% of the emails through.

But browsers certainly have gotten better since then. The major browser vendors, including Google and Microsoft, continue to add security features that can flag potentially dangerous emails. In the past many of the early browsers had multiple confusing security settings: now most just have a simple “protect me from dangerous sites” on/off switch to make it easier, and it is often turned on by default.

Google has also stepped up its own security efforts. For example, Google’s Advanced Protection program adds multi-factor authentication and limiting third-party application access to your account.And earlier this summer Google made changes to the way it handles browser plugins, adding new warnings for users and a more involved verification system for apps that will hopefully detect when an app seems suspicious. This was in response to an app that was called “Google Docs” but turned out to be malicious. Google has had its Safe Browsing technologies for more than a decade, and continues to beef up its warning messages and scrutiny on phished and other dangerous emails using this system too.

It is a cat and mouse game to be sure. As the bad guys get better at sending plausible emails, the security vendors have to continually up their game to find them.

Browsers aren’t the only defensive posture. A number of vendors (such as KnowBe4, Phishing User Training, PhishMe, Wombat Security and MediaPro, among others) offer **phishing simulation training and awareness programs**. These work by sending out messages that could be phishing attacks, but have been neutralized in advance, in the hopes that users will learn how to detect the real attacks in the future. IT managers get a scorecard of who missed which message, with the goal to not shame users but to help them learn from their mistakes. These simulations seem to work, with phishing success rates dropping: clearly, users can learn how to be more resilient. But they still can’t cover every situation, and users may forget their training when out in the field, rushing to read their messages.

A third series of technologies are **email gateways or other email-centric protective mechanisms**. Products such as Barracuda, Sophos, CloudMark and others have been around for years, mainly filtering out spam messages and lately doing more about phishing as well. These can be used in a variety of different places on the network: as email firewalls, as reverse proxies, or as plug-ins to email SaaS providers such as Microsoft’s Office 365. The latter is where Inky’s Phsh Fence technology fits in. Let’s take a closer look at what they are doing.

What Phish Fence does

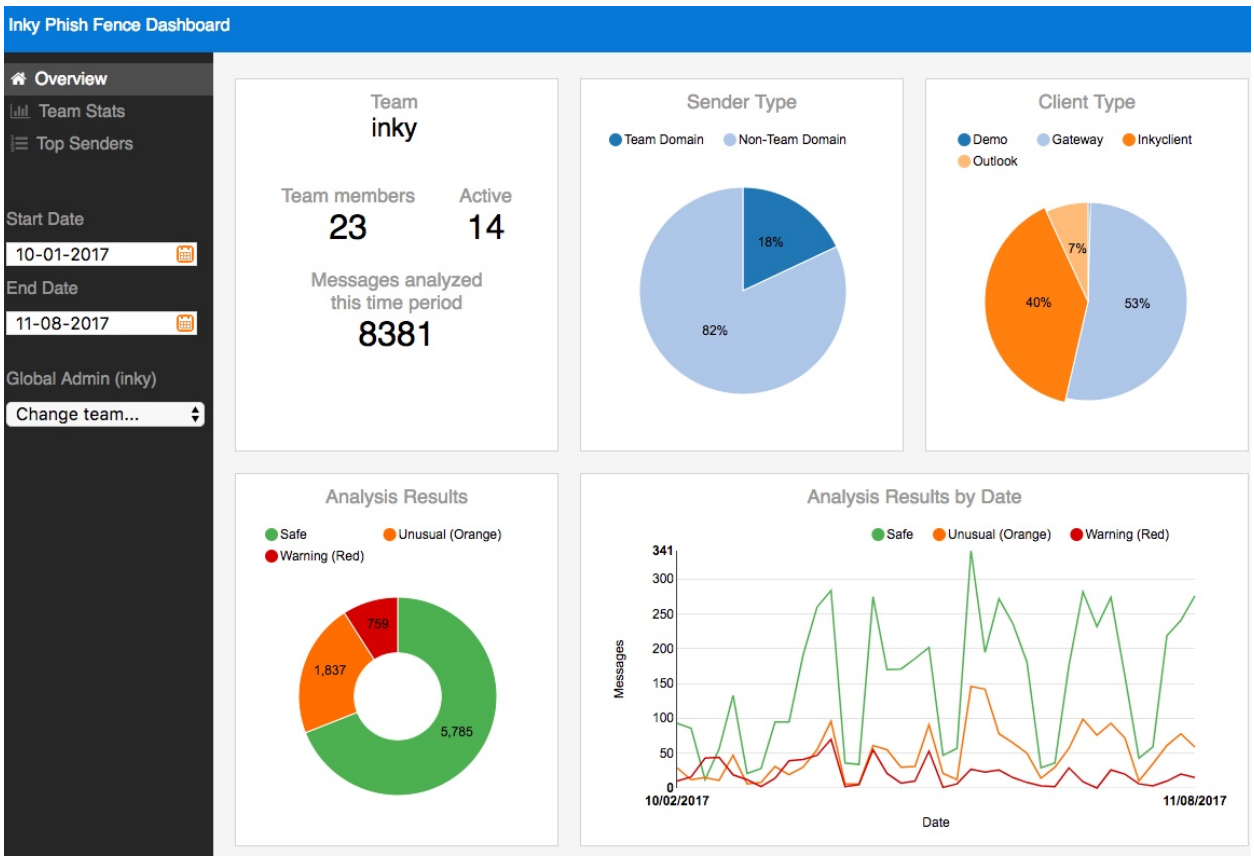
All of these defensive methods have their limitations though, and depend on interpreting the stream of emails to find the potential phished content. Unlike some of its competitors, Phish Fence is a complete software solution that tries to make users smarter about the content of their email messages. It uses an add-in to Google's G Suite or the online Exchange servers as part of Microsoft's Office 365 cloud-based services. It is not an email filtering solution: you still get **all the emails intended** for your inbox. But it augments what you see as you are browsing your messages, in a way that you can act on each email that it deems to be suspect, and do so while you are processing each message in your inbox.

There are both free and paid versions of Phish Fence. The free versions work with Outlook.com, Hotmail and Gmail accounts and have add-ins available both from the Google Chrome Store and the Microsoft Appsource Store. These versions require the user to launch the add-in proactively to analyze each message, by clicking on the Inky icon above the active message area. Once they do, Phish Fence instantly analyzes the email and displays the results in a pane within the message. The majority of the analysis happens directly in Outlook or Gmail so Inky's servers don't need to see the raw email, which preserves the user's privacy.

The paid versions analyze every incoming mail automatically via a server process. Inky Phish Fence can be configured to quarantine malicious mail and put warnings directly in the bodies of suspicious mail. This means users don't have to take any action to get the warnings. In this configuration, Outlook users can get some additional info by using the add-in, but all the essential information is just indicated inline with each email message.

I produced a short video screencast that shows the differences in the two versions and how Phish Fence works.

Regardless of which version, Phish Fence is zero-administration, requiring no migration or changes to backend data-loss prevention, e-discovery, or other related systems. The enterprise version includes a dashboard that shows threat origins and types, as shown below.



Phsh Fence does not intermediate mail delivery, eliminating lost emails, outages, and delays common to gateway email security solutions. Many of the email filtering services -- including the built-in tools for GMail -- just scan and segregate your messages, moving anything suspect to a special folder where you still have to process your mail and make sure it is legit. Phish Fence leaves your messages in your inbox, where you can act on the intelligence information that it has collected.

As you can see from our descriptions of the numerous phishing methods above, understanding when a potential email isn't quite right requires weighing a variety of risk factors, such as:

- Does the sender's credentials match their actual domain address?
- Is there a URL that points to a questionable location or uses unusual characters, such as a typosquatted or homographic domain?
- Is the sender using a verified identity (such as with DKIM tools) or trying to impersonate a well-know brand?
- Is the sender trying to imerpsonate a particular person or use stolen credentials?
- Is the subject line suspicious?

- Is there sensitive content in the message body that should be flagged, such as mentioning passwords, personal identities or money transfers?

Phish Fence then scores the message according to a machine learning algorithm that is similar to what Facebook uses for face recognition, only for brand logos and other images. The algorithm also looks at the above issues and classifies each message into three levels and shows the appropriate colored warning:

- 0 clean (no warning)
- 1 suspicious; something about the message is unusual (orange warning)
- 2 malicious; Inky is pretty sure this is a malicious forgery

We tested Phish Fence with a variety of simulated phishing attacks, using a combination of well-known exploits and picking some new emails and URLs from PhishTank and other similar collection services. We found Phish Fence flagged all exploits accurately and gave warnings that matched the messages. We can't guarantee that Phish Fence will catch every attack, but it certainly seems well-designed to prevent the most common forms of phishing that have been used over the past several years.

Conclusion

Phishing is a big problem and one of the main sources of entry into enterprise networks. Hackers continually improve their methods to compromise email messages and prey on distracted users to get their malware introduced into a system. Inky's Phish Fence provides a pro-active defense against most of the common forms of phishing and can be a great protective tool for small and large enteprises alike.

About Inky (@inkymail)

Headquartered in Rockville, Maryland, Inky makes the Inky Enterprise Suite of identity-based cryptography security and email products. Inky was founded by Dave Baggett. Prior to Inky, Baggett was a co-founder of ITA Software, an airfare search company that sold to Google in 2010 for $730 million. For more information, please visit inky.com.