MARCH 2020

CYREN

CYBERTHREAT Report

The Phishing Issue

From Targeted Attacks to Evasive Phishing

TABLE OF CONTENTS

Phishing on the Rise in Business Seas 3

The Anatomy of a Phishing Attack 4

Understanding Phishing Terminology 5

How Business Email Compromise Reels in the Big Catch 6

Evasive Phishing Driven by Phishing-as-a-Service 9

The Top 6 Evasive Phishing Techniques 10

Inbox Detection & Response: A New Vision for Email Security 11

Exploiting CAPTCHA: The Latest Evasive Phishing Tactic 12

Financial Phishing: Still a Major Problem 13

Why Trusted Brands Can't Always be Trusted 14

Industry Case Study: Real Estate is the Perfect Target for Phishing 15

Phishing Sites Don't Last a Zero Day 17

What Companies Can Do to Improve Protection 18

Phishing on the Rise in Business Seas

> “Phishing attacks are growing exponentially. We need a response.”

In the last year, the number of active phishing URLs being monitored by Cyren's global security cloud has grown to over 12 million, representing an increase of approximately 100,000 URLs each month. To be clear...this is net growth. Consensus estimates are that, on average, 1.5 million new phishing websites are created every month, and studies show that half of these URLs have served their useful life and are already inactive within 24 hours, as phishing campaigns are aggressively managed by the phishers. (You can read more on p.16 about zero-day phishing sites.)

The reality is that phishing is not going away. Research from government agencies and IT industry analysts demonstrates that phishing attacks are successful: last year the FBI Internet Crime Complaint Center reported a 100% rise in business email compromise attacks; Osterman Research reported 48% of organizations have suffered a phishing-related breach; and Verizon reported phishing was the top threat variety resulting in a breach.

Phishing is on the rise for several reasons—most fundamentally because it works. Phishing provides a robust ROI to the criminal gangs behind it, as barriers to entry have fallen and the “phishing-as-a-service” economy has evolved to lower costs and make it possible for even the non-technical aspiring criminal to get into the game. We also can't lose sight of the fact that phishing's primary distribution channel—email—is the easiest and only reliable way to reach business users directly.

Cyren is uniquely positioned to observe, analyze, and halt phishing attacks as they happen. In this updated phishing issue, we explore recent trends in phishing, provide insight into the latest tactics phishers are using to evade detection, and discuss why some industries are more at risk than others. To begin to stem the increasingly negative impact of phishing, companies must recognize that no single security control is 100% effective and take a defense-in-depth approach to email security. The massive move to hosted email solutions over the past couple years, Office 365 most notably, has created an opportunity for a new layer of security at the inbox. Read on to understand how to leverage that opportunity.

Dr Richard Ford
Chief Technology Officer
Cyren

The Anatomy of a Phishing Attack

While most folks know what phishing is, few realize the lengths to which a criminal will go to initiate a phishing attack. More than just distributing emails with fake corporate logos like LinkedIn or Facebook, cybercriminals design attacks carefully by using fake clickable advertising, spoofing well-known online brands, and creating legitimate-looking phishing websites to capture the sensitive data that the unsuspecting victim enters.

STEP 1 VICTIM IDENTIFICATION

Mass Phishing Attack
- Untargeted, large group of victims.

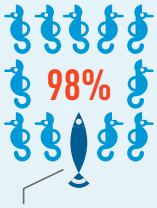
Targeted Phishing Attack
- Specific group, or high profile victim.

32%

Breaches involving phishing, according to the 2019 Verizon Data Breach Investigations Report.

STEP 2 SOURCE SETUP

Brand Names
- Phisher selects a brand name for mass email distribution, such as Apple, PayPal, or Dropbox
- Using a newly created domain or a hacked website, hacker builds webpages that resemble the one for the trusted brand name.

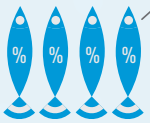


98%

98% of phishing website URLs target name brands such as Apple, PayPal, Dropbox, Google, and Microsoft

Sophisticated Content
- Phisher develops an email with legitimate-looking content such as legal or financial information.
- Spoofs the email address of someone at the target organization or of a known contact to the target.

STEP 3 DISTRIBUTE ATTACK



40%

A 2019, Osterman Research report found 40% of organizations had Office 365 credentials compromised.

Mass Distribution
- Phisher sends a mass distribution email containing brand logos/name and links to fake webpages.
- Places links to fake web pages in banner ads, on social media, or in text messages.

Targeted Distribution
- Phisher sends email to specific target victim or group.

STEP 4 HOOK VICTIMS

Click Fake Links
- Victims click on link in the email and enter sensitive credential information into fake web page.

Respond Directly To Email Request
- Victim responds directly to email with requested information, such as login credentials or financial information.

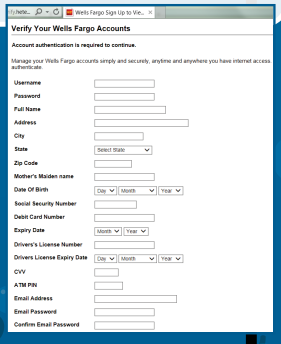
#1

Phishing, as ranked in top threat action varieties in breaches.

#2

Use of stolen credentials, as ranked in top threat action varieties in breaches*

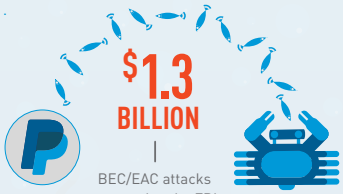
*SOURCE: 2019 Verizon Data Breach Investigations Report



STEP 5 EXPAND OR MONETIZE

Develop Additional Attacks
- Phisher uses stolen credentials for the next phase of the attack (such as an APT).
- Collects additional email addresses from hacked accounts for future attacks.

Financial Gain
- Phisher sells the stolen credentials on the black market.
- Phisher steals money using credentials from bank, PayPal account, or fake wire transfer.



$1.3 BILLION

BEC/EAC attacks reported to the FBI increased 30% over the previous year and adjusted losses increased 90% from $675m to 1.3B

Understanding Phishing Terminology

THREAT TYPES

PHISHING

A homophone of the word 'fishing,' phishing is an attempt to entice a person into providing sensitive or confidential information which can be used or monetized by cybercriminals. In a phishing scam, criminals distribute electronic content to a series of victims. The content uses social engineering tactics designed to trick the user into engaging in a particular activity, such as clicking a link or responding to the email. The victims, thinking the content is real, provide the phisher with personally sensitive information such as usernames, passwords, banking, financial, and/or credit card details. Methods of phishing distribution include email, online advertising, and SMS.

CLONE PHISHING

A phishing attack in which the 'phisher' uses a genuine, previously delivered email to create an identical (or almost identical) email containing similar content, attachment, recipient, and sender email address. A fraudulent link or attachment replaces the original one. Because the email appears to come from a legitimate source, this spoofed email is used to gain trust with the victim.

SPEAR PHISHING

A targeted phishing attack focused on a specific person or group of people and often involves research and spoofing of the sender name and e-mail address. Blocking these types of attacks usually requires "imposter protection" security capabilities.

WHALING

A form of spear phishing targeting senior corporate executives or high-profile individuals such as those in government. Called whaling because the target is considered higher-value than a regular employee, and the information being stolen is significantly more valuable.

BUSINESS EMAIL COMPROMISE (BEC)

Often called CEO fraud because the attacker sends emails impersonating the CEO or other senior individual. The recipient will likely be a more junior staff member. The email will use social engineering tactics to convey a sense of urgency and coerce the recipient into performing an action. This action will likely involve wire transfers to accounts controlled by the attacker, the purchase and transfer of other items with a monetary value, such as electronic gift cards, or a request for sensitive information that can be used for financial gain, such as personnel files.

EMAIL ACCOUNT COMPROMISE (EAC)

A BEC attack will be most effective when launched from the impersonated sender's genuine email account. This will likely have been compromised by an earlier phishing email and is referred to as an Email Account Takeover (EAC) attack. Once completed, the attacker can login to the compromised account and silently monitor communications ready to launch the next stage of the attack. .

How Business Email Compromise Reels in the Big Catch

In the world of phishing, there are two types of "phishers:" those that use their nets to scour the ocean and capture as many victims as possible, and those that use a single rod and reel to catch the big haul trophy—the corporate executive, government official, celebrity, or other high-profile individual. This sophisticated and targeted form of phishing—called spear phishing or whaling when directed at high-level business executives—is on a dramatic upswing.

Spear phishing in the form of business email compromise (BEC) attacks have been increasing in number over the last few years, driven by their relative success rate compared to other financially motivated attacks. The most recent FBI Internet Crime Report, published in 2019, stated that BEC/EAC attacks reported to the FBI had increased 30% over the prior year, while adjusted losses increased a massive 90%, from $675M to 1.3B. An increase is also suggested in the Verizon Data Breach Investigations Report, which states that senior executives are 12 times more likely to be the target of a social incident than the previous year.

Security researchers find that BEC attacks often take two forms: (1) A multi-phase attack, in which the attacker has gained access to the actual target's email account. Protection from this type of threat requires upfront URL protection so the phishing link doesn't arrive in the victim's inbox in the first place. (2) Email spoofing, which involves the attacker manipulating the names in the email fields or faking a corporate website domain to make it appear as if the email arrived from an internal or familiar external source. Protection from email spoofing requires email security that has an 'imposter detection' component, which is able to flag and block a spoofed email account or domain.

MULTI-PHASE SPEAR PHISHING

THE SCENARIO

In the latest BEC trend, cybercriminals are using social engineering to attack targets in multiple phases. Rather than engaging in a full assault at the onset with a fake request for corporate passwords or financial information, cybercriminals are now taking a little more time and slowly infiltrating an organization, first for reconnaissance and then to build the foundation for an attack that looks legitimate.

HOW IT WORKS

STEP ONE: infiltration using scare tactics—Imagine you're a mid-level employee at a small- to medium-sized corporation and suddenly you find an email in your inbox telling you that your corporate Office 365 account is temporarily suspended because your password is expired and your email address needs to be reactivated. You click the link and it takes you to a web form on what looks like the Microsoft Office 365 site. You're asked to provide your corporate email address and current password, as well as other personal information such as company name and title, in order to reactivate the account.

Given employees' dependence on email, they are frequently highly motivated to avoid any possible interruption. And, frankly, for better or worse, today most employees are accustomed to receiving requests to update their passwords, making the fake 'deactivated email account' technique a fairly common and successful ploy. It's also not a direct pitch for financial records or credentials, which (for some) immediately raises a red flag. Criminals also know that robust cybersecurity services, as well as two-factor authentication, are not in use as often at small- to medium-sized businesses.

Block at the Beginning

The primary way to block a multi-phase spear phishing attack is at its start—with the original URL that arrived via email requesting, for example, an Office 365 email password. Security services should stop users from accessing phishing URLs with immediate "time-of-click" analysis and blocking, as well as with protection that identifies and blocks just-released "zero-day" and previously unknown phishing links based on the correlation of data across transactions.

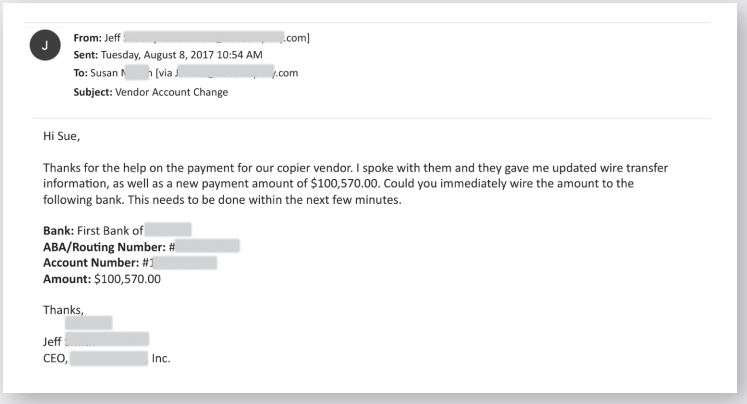
HOW BUSINESS EMAIL COMPROMISE REELS IN THE BIG CATCH

continued from previous page

STEP TWO: infiltration survey & exploration—Armed with your corporate login and password, the criminal can now survey the landscape, reading your email to learn more about the organization and get details about who you work with, who your customers are, the names of decision-makers, who manages HR data, who controls the finances, etc.

STEP THREE: launch attack—Having these details enables the criminal to launch an effective spear phishing attack. For example, using your email address, the criminal might send an email to your team member in accounts payables, who you've been working with to get one of your vendors paid. The email might look something like the example on the right.

Because the email arrives from a legitimate internal account, the targeted employee responds by initiating the wire transfer.



From: Jeff [redacted].com]
Sent: Tuesday, August 8, 2017 10:54 AM
To: Susan [redacted] [via J[redacted].com
Subject: Vendor Account Change

Hi Sue,

Thanks for the help on the payment for our copier vendor. I spoke with them and they gave me updated wire transfer information, as well as a new payment amount of $100,570.00. Could you immediately wire the amount to the following bank. This needs to be done within the next few minutes.

Bank: First Bank of [redacted]
ABA/Routing Number: #[redacted]
Account Number: #1[redacted]
Amount: $100,570.00

Thanks,
[redacted]
Jeff [redacted]
CEO, [redacted] Inc.

This email arrives from a real—but compromised internal account—making the scam more likely to succeed.

EMAIL SPOOFING

THE SCENARIO

Email spoofing is similar to the multi-phase example mentioned previously, in that an email arrives in an recipient's inbox appearing as if it came from an internal source, such as the CEO or another executive, or a well known external source, such as a vendor, accountant, or lawyer. However, in these instances, the email account itself has not been compromised. Instead the attacker "spoofs" the sender's email address or website domain to make it appear as if the email came from a known source.

The success of these attacks is based on the simplicity of the email that is sent. It will contain no malware, no attachment, and no links, all of which are traditional threat signs. Imposter email attacks are typically low volume and targeted, rendering most defenses that rely on traditional email threat detection methods useless. The attacker ensures maximum success by hand-crafting each email to appeal to the target recipient.

With no malware or attachments, endpoint detection will likely not identify and block the threat. That leaves the unsuspecting recipient in the finance team as your last line of defense.

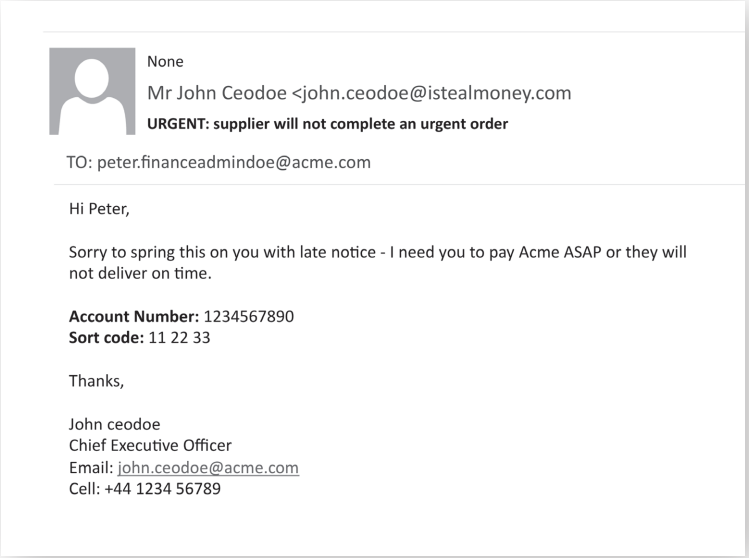
HOW BUSINESS EMAIL COMPROMISE REELS IN THE BIG CATCH

continued from previous page

HOW IT WORKS

Your finance administrator has just received an email from the CEO telling him to send money to a vendor, so that they can deliver an urgently needed service or a product, and it needs doing NOW. How much time should he spend trying to decide whether the email is a threat or not? How much training is enough? And how much reliance can a business realistically place on non-technical users?

Some impostor emails are easier to recognize than others. For example, simply hovering over or clicking on the actual sender email address to ensure it matches the CEO's email address, rather than relying on the "from" field, will quickly demonstrate whether an email is legitimate or not. However, this assumes that the recipient takes the time to actually hover over the email address to verify authenticity, instead of instantly reacting to a "CEO request" to get something done asap.



None
Mr John Ceodoe <john.ceodoe@istealmoney.com
URGENT: supplier will not complete an urgent order

TO: peter.financeadmindoe@acme.com

Hi Peter,

Sorry to spring this on you with late notice - I need you to pay Acme ASAP or they will not deliver on time.

Account Number: 1234567890
Sort code: 11 22 33

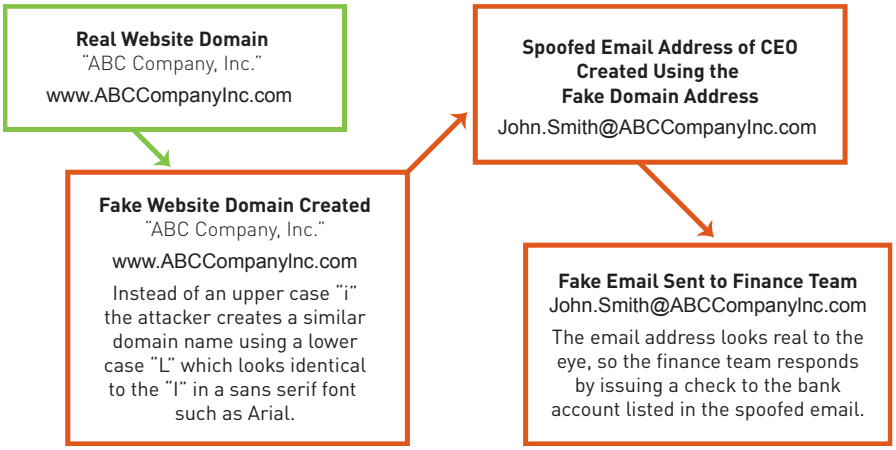
Thanks,

John ceodoe
Chief Executive Officer
Email: john.ceodoe@acme.com
Cell: +44 1234 56789

An example of what a spoofed email might look like.

IDN HOMOGRAPH ATTACK OR SCRIPT SPOOFING

More difficult to spot are attacks involving lookalike domains, also sometimes called an internationalized domain name (IDN) homograph attack or script spoofing. These attacks require a bit more effort from the attacker, who registers an email domain that reads like the target company's. It might be the same, except for a single character that has been replaced, dropped, or added. The CEO's name is then used to create a legitimate email address on this similar domain. The result is that all email fields appear valid, with the sender's name and email address seeming to match, but on closer inspection, they belong to a domain that just resembles the recipient's company's own.

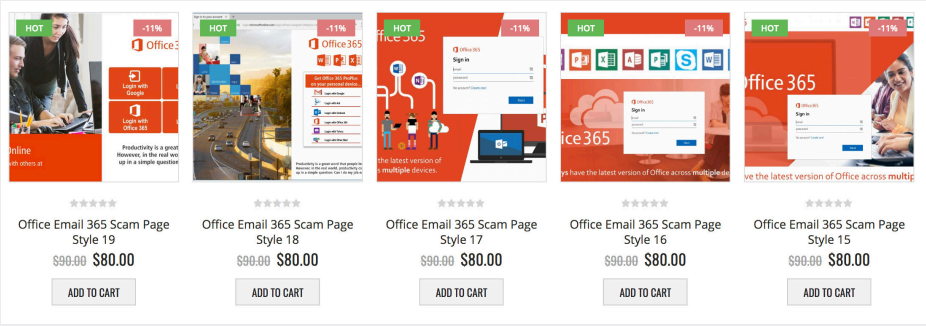


Solve the email spoofing problem and keep users productive

Protecting from email spoofing requires an imposter detection capability that is fully integrated with existing email security. It should examine all of the email fields, including the subject and body text to look for the tell-tale signs of social engineering, as well as an examination of the email domain to determine whether there might be a close match with the company's own. It should also allow for input of a list of those users whose addresses an attacker might try and spoof. When the results of all of these tests are correlated, this impostor detection capability should determine the likelihood that an attack is underway and quarantine or tag emails as appropriate, based on this likelihood.

Evasive Phishing Driven by Phishing-as-a-Service

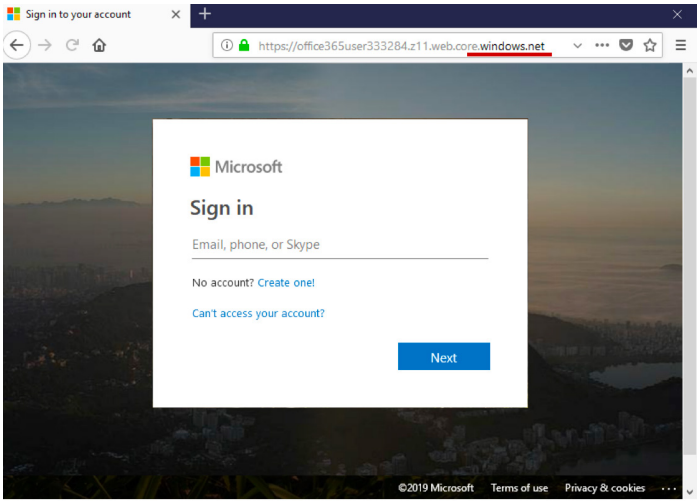
The phishing-as-a-service industry is making easy-to-use phishing attack tools and even full campaigns available at cheap rates, with full-service subscription prices typically varying from $50 to $80 per month, depending on the level of service, and realistic phishing web kits available for download for as little as $50. In the first half of 2019, Cyren's research lab turned up 5,334 new, unique phishing kits deployed to the web, an indication of the scope and scale of turn-key phishing offerings.



Different style scam pages targeting Office 365 credentials on offer from a Phishing-as-a-Service web site—and with a $10 discount!

PHISHING-AS-A-SERVICE IS EMBEDDING EVASIVE PHISHING ATTACKS

A straight line can be drawn between the availability of such kits and turn-key phishing platform services and the growth in evasive phishing—phishing attacks that use tactics to confound detection by email security systems. Today's reality is that we are seeing more evasive phishing campaigns in the hands of more attackers at less effort and lower cost than in the past. This is due to technically sophisticated phishing attack developers adopting a SaaS business model to let even the most amateur criminal wanna-be spoof targeted web sites with a high degree of authenticity and embedded evasive tactics.



Fake Microsoft log-in page fools even discerning users with legitimate windows.net domain and legitimate SSL certificate

87% OF PHISHING KITS INCLUDE EVASIVE TECHNIQUES

Cyren's security lab found that 87 percent of phishing kits sold on the dark web include at least one type of basic evasive technique. One expectation for the future is that phishing developers will begin to combine many techniques together, as we've seen with malware. One piece of malware did 26 different checks to try and avoid detection—we expect phishing to continue to evolve in this direction, with layers of detection evasion techniques being used.

METHODS FOR THE MADNESS

Much like the evolution of evasive malware tactics over the past 30 years, professional phishing developers are utilizing more methods to fool automated defenses, and are including those methods in pre-packaged campaigns and phishing services made widely available on the dark web.

The Top 6 Evasive Phishing Techniques

MOST COMMON EVASIVE PHISHING TECHNIQUES

1. **HTML character encoding**
2. **Content encryption**
3. **Inspection blocking**
4. **URLs in attachments**
5. **Content injection**
6. **Legitimate cloud hosting**

HTML character encoding—in this ruse, some or all of a phishing page's HTML code is encoded and is displayed normally by web browsers, but security crawlers looking through the code will not be able to read the content, missing keywords associated with phishing like "password" and "credit card" in an example from a spoofed PayPal site.

Content encryption—a tactic similar to encoding, because the content in the code does not show as readable text. But here, rather than changing the representation of a word with character encoding, the entire content is encrypted, and a key is needed to decrypt it. The encrypted file usually looks very small, but when decrypted, often done by a JavaScript file, we see the real content.

Inspection blocking—the technique most regularly incorporated into phishing kits, phishers employ block lists for connections from specific IP addresses and hosts known to be used by security companies. This prevents security technology and human analysts from evaluating and seeing the true nature of a phishing site and blocking access by security bots, crawlers or other user agents that are searching for phishing sites, like the Googlebot, Bingbot, or Yahoo! Slurp. When someone on the block list tries to access the page, they are usually presented with a "404 page not found" message.

URLs in attachments—a growing phishing trend over the past year has been to not place links in the body of emails, but instead hide them in attachments, in order to make detection more difficult. A typical example might be a simple PDF constructed of images and made to look like a OneDrive document, with a single button that links to a phishing site.

Content injection—this is not a new technique, but a tried and tested method used to lull the user and complicate detection by changing a part of the content on the page of a legitimate website. The unsuspecting user is then taken to the phishing page, outside the legitimate website.

Legitimate cloud hosting—this is a tactic that has grown significantly recently. By hosting phishing websites on legitimate cloud services, like Microsoft Azure, phishers are able to present legitimate domains and SSL certificates, lulling even the most attentive user into thinking a given phishing page is trustworthy. Further, many security vendors whitelist certain domains.

Phishing is getting through

The impact on organizations everywhere is quite clear.

According to survey data from Osterman Research, in 2019, **48%** reported a successful email phishing related breach. This increased from **44%** in 2018 and **30%** in 2017.

Inbox Detection & Response: A New Solution for Evasive Phishing

Since the early days of anti-spam software, email security architecture has evolved over time in response to new challenges. Today's sophisticated evasive threats are too frequently evading today's security measures, so new approaches are needed.

Most companies today have deployed a Secure Email Gateway (SEG) appliance or cloud service. Detection technologies used by the SEG now include integrated sandboxes to protect from zero-day threats, time-of-click analysis to defend against embedded URLs that are weaponized post-delivery, and authentication protocols such as SPF, DKIM and DMARC help detect impersonation attacks.

THE LIMITATIONS OF THE SEG

But the SEG has a major limitation – it protects only at a single point in time, at time of delivery, or in the case of time-of-click protection, when the user clicks the link.

In a world of evasive phishing and malware threats, the one-pass detection provided by the SEG is not enough. You need to deploy a defense-in-depth email security architecture. The SEG has its place in this approach. It provides solid front line security to block spam, known threats and when you introduce advanced detection capabilities like sandboxing, some unknown threats. Where the SEG falls short is detecting highly evasive phishing, spear phishing, BEC and cousin domain spoofing, and sitting at the gateway, it can do nothing to detect compromised email accounts.

A NEW LAYER OF EMAIL SECURITY – INBOX DETECTION & RESPONSE (IDR)

What is required is an email security architecture designed specifically to detect today's threats. Cloud platforms like Office 365 make this possible. They provide APIs that enable you to deploy security directly into the mailbox. This emerging category of product is called Inbox Detection & Response (IDR).

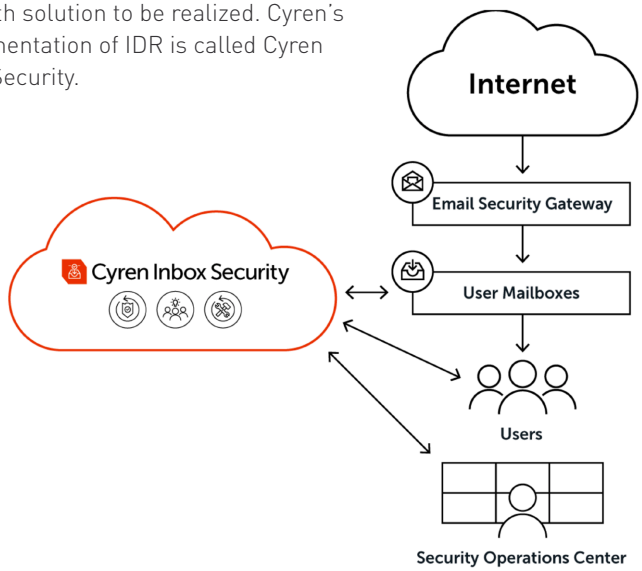
IDR can protect against new threats by continuously monitoring every user's mailbox. It can track behaviors and user interactions in the mailbox, and identify anomalies. If a new threat is discovered at any time, IDR can automatically delete every copy across every mailbox. This automatic remediation removes the burden on the security analyst and reduces cost to respond.

IDR can also provide a framework for users to interact with detection technologies, incorporating user feedback quickly and automatically to identify and protect against phishing attacks. Data collected through the framework can be correlated to determine whether an email is malicious and action should be taken. Incident and case management workflows can eliminate false positives and help email admins and security analysts identify threats for further investigation.

Finally, IDR can create a fast feedback loop to reinforce machine learning algorithms. This uses the outputs captured by continuously scanning emails, monitoring user behaviors, and tracking URLs. Through analysis of this data, IDR can better detect anomalies, predict what the next threat might look like and push intelligence to SEGs and other security assets, strengthening your organization's security posture as a whole.

ADD IDR TO CREATE EMAIL SECURITY DEFENSE-IN-DEPTH

IDR brings continuous monitoring, detection and response to email security, using technology that cannot be deployed at the SEG. In turn, the SEG provides technologies that cannot be deployed in the inbox, so it will continue to play a role as part of your email security stack. Finally, there are technologies that can be deployed at the gateway or in the inbox, allowing a true email security defense-in-depth solution to be realized. Cyren's implementation of IDR is called Cyren Inbox Security.



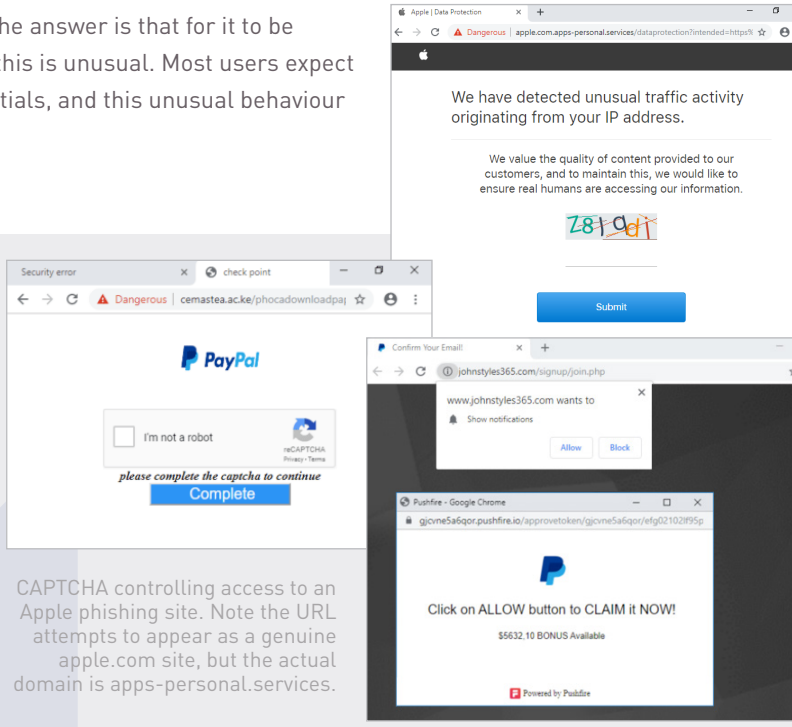
Exploiting CAPTCHA: The Latest Evasive Phishing Tactic

The Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) has been used in commercial applications since the early 2000s. As its name suggests, it is a mechanism for ascertaining that a real human is performing an action at a web site. CAPTCHA is generated by distorting letters and numbers in such a way that a computer using OCR cannot resolve it. Typical applications were originally centered on authentication. For example, if you enter an incorrect password multiple times, you might be presented with a CAPTCHA to ensure that a bot is not attempting to brute force a login. Today there are other applications, such as preventing bots automatically posting good product reviews to falsify scores on review sites.

HIDING PHISHING SITES BEHIND CAPTCHA

Phishing evasion tactics have evolved over time, each a new attempt to thwart cyber security companies, who, in turn, evolved their detection techniques. The latest tactic Cyren's security analysts are seeing on the increase is extremely simple. If you don't want security companies' automated crawlers, bots and user agents to be able to access your phishing page, simply control that access using a mechanism devised specifically to block computers – CAPTCHA. Like the use of block lists, if the phishing page cannot be reached, even the best detection engine cannot do its job.

If it is so simple, one might ask why it has not been widely used. The answer is that for it to be successful, it has to be presented prior to the phishing page, and this is unusual. Most users expect a CAPTCHA to appear on the same page as the request for credentials, and this unusual behaviour might lead perceptive users to realize they are being phished.



CAPTCHA controlling access to an Apple phishing site. Note the URL attempts to appear as a genuine apple.com site, but the actual domain is apps-personal.services.

PHISHERS ARE USING MULTIPLE CAPTCHAS

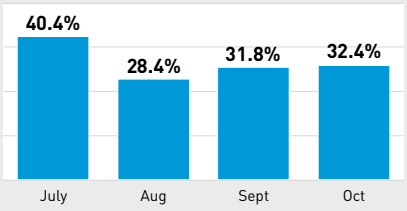
CAPTCHA has evolved over the years, with projects dubbed reCAPTCHA created to improve security and reduce user friction. Techniques now include a simple checkbox, clicking images that include specific objects, and tracking human-like behaviors. The latter requires no human intervention at all, so is not an appropriate evasive phishing technique, but Cyren's security lab have seen all other variants. This makes life even more difficult for cyber security companies, who have to figure out how to defeat each of the tactics in use. Here are a few examples found recently by Cyren's security analysts.

When a cyber security company's bots, crawlers or analysts come across phishing evasion techniques, their very existence raises suspicion. For example, if a security bot attempts to access a suspected phishing page and is blocked, because its IP addresses are included in the phisher's block lists, that very behavior is noted as potentially suspicious. The next step in this situation might be to access the page from an IP address unknown to the phishers, and if a different response is received, suspicion is increased significantly. Before discovering this new CAPTCHA evasion tactic, reaching a CAPTCHA page was not deemed suspicious, but now detection has evolved to understand how this combines with other attributes of the attack, to ensure that users are protected.

Financial Phishing: Still a Major Problem

The dramatic increase in tax and financial phishing schemes seen over the last few years has slowed, but they are not going away.

Cyren's security lab monitors trends in financial phishing schemes. Unsurprisingly, these make up a large proportion of the total phishing URLs we track. We see an abundance of phishing scams designed to steal more than just credentials, and some are really quite audacious, requesting anything from answers to online security questions through to credit card numbers.

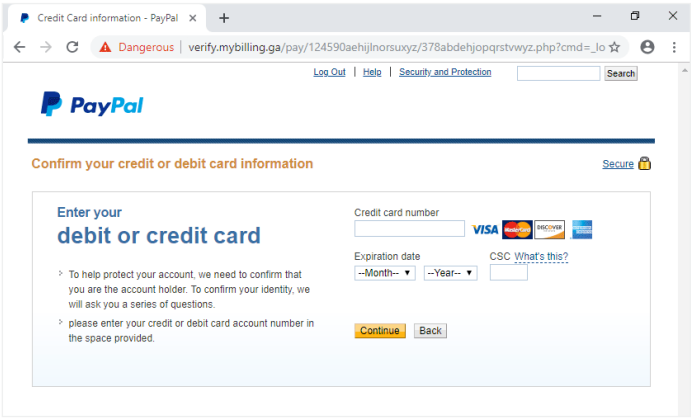


Financial phishing comprises a major proportion of phishing sites tracked.

TOP 10 PHISHED FINANCIAL BRANDS

1. PayPal
2. Bank of America
3. Wells Fargo
4. CIBC
5. Chase
6. Farmers State Bank
7. BMO
8. USAA
9. SunTrust Bank
10. American Express

The number one financial brand we tracked was Paypal, and the majority of those in the top 10 are, unsurprisingly, the world's largest and well-known financial brands.

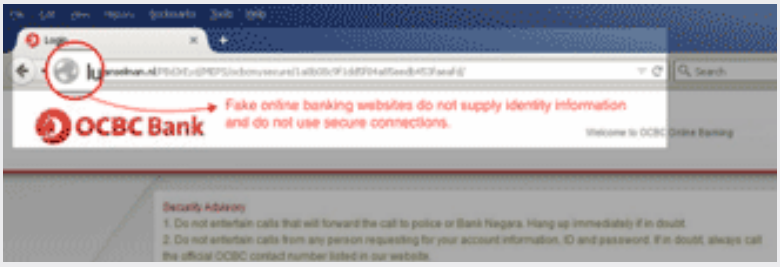


THINK BEFORE YOU CLICK! PREVENT FINANCIAL PHISHING

Implementing strong email gateway security can prevent both large-scale and localized phishing emails from reaching users in the first place. Email gateway security also blocks access to phishing links as a second layer of protection.

In addition, other ways to protect yourself and your company from financial and tax phishing fraud include:

- Type the address of your financial institution directly into your web browser.
- If you've accidently clicked a potential phishing link in an email, check the URL to see if it displays the financial organization's name, along with the "lock" icon to indicate you are using a secure connection.
- Enter fake credentials to see if you are rejected. Fraudulent online banking websites will typically just accept any login credentials and then redirect the user to more phishing pages to collect other types of sensitive information. Legitimate banking sites will automatically recognize the fake credentials and display a message that says the user name and password are incorrect or cannot be found.



A fake online banking login page will not supply a security login icon or a correct URL address.

Signed and verified online banking login page.

Why Trusted Brands Can't Always be Trusted

Internet platforms, financial, and shopping brands are still the most popular targets for phishing, according to the most recent phishing trends.

To learn which brands were the most frequently targeted by phishers, Cyren analysts extracted about a million URLs classified as phishing during Q3. There were very few surprises and the top 20 contained almost all the same brands as our previous report, in which we used data from Q1 of 2018. There was one very conspicuous change - IRS.gov does not feature, because clearly tax fraud is only a valid activity in Q1, tax season.

This selection of online brands by phishers provides a useful indicator of phishing motivation:

- **Financial sites are clearly targets because stolen credentials provide criminals with direct access to money and/or bitcoins, in addition to login credentials that could be resold on the black market.**
- **Online services, such as Apple, Google, and Microsoft serve as an 'Attack Platform' for cybercriminals; stolen credentials from a list of Gmail or Apple subscribers can be resold or possibly used to hack other websites, since many people use the same credentials (user names & passwords) for login on multiple sites. Additionally, email or social media logins can be used to target contacts of the victim.**
- **Shopping or commerce websites, such as Amazon and Alibaba offer criminals both credential information and the possibility of online shopping sprees or financial data if the victim stores credit card or banking information with the online services.**

Brand	% phishing URLs
Apple	21.2%
PayPal	10.2%
BankofAmerica	6.0%
Facebook	3.0%
Chase	2.9%
Microsoft	2.5%
CIBC	2.4%
Google	2.1%
WellsFargo	2.0%
DHL	0.9%
Farmers State Bank	0.8%
Amazon	0.8%
Dropbox	0.7%
Yahoo	0.4%
AOL	0.4%
Netflix	0.3%
Adobe	0.3%
eBay	0.3%
SunTrustBank	0.3%
AmericanExpress	0.2%
Other	42.3%

Industry Case Study: Real Estate is the Perfect Target for Phishing

The days of "spray and pray" cyber attacks, where generic phishing emails or emails with malware attachments were sent to massive mailing lists are not completely gone, but cyber criminals have, for many years, reaped rewards from highly targeted attacks. This was the case with malware, and phishing has followed the same course.

TARGETING THE RIGHT INDUSTRY WITH THE RIGHT ATTACK

Targeted attacks have existed for many years. In 1989, at a time when malware was primarily about computer geeks gaining kudos for creating havoc rather than financial gain, the AIDS ransomware was named such because it specifically targeted AIDS researchers.

In the latest Verizon Data Breach Investigations Report, phishing is included in the crimeware category. Public sector organizations reported by far the most incidents and the highest number of breaches related to crimeware. The difference comes when we look at the percentage of incidents that led to a breach – just 1.4% for the former but a massive 63.6% for real estate. This is likely related to the highly targeted nature of the attacks on the latter and the tactics used.

BUSINESS EMAIL COMPROMISE (BEC) IS THE ATTACK OF CHOICE FOR THE REAL ESTATE INDUSTRY

A house is by far the largest financial transaction undertaken by most individuals in their lifetime. It is also something done infrequently, if not just once, making the whole process new and often confusing for the home buyer. No wonder then that tapping into the flow of payments from buyers to sellers is a major objective for criminals wanting to make big bucks. Increasingly, BEC is the weapon of choice, and everyone involved in the transaction is a target for compromise – the buyer, the seller, the agent and the lawyers.

THE REWARDS ARE WORTH THE EFFORT

The goal of the attack is always the same – get the buyer's payment transferred to a bank account controlled by the criminal. The 2019 FBI Internet Crime Complaint Center (IC3) report provides a number of examples.

A BEC victim in New York received a compromised email from their agent during a real estate transaction and wired $50,000 to a fraudulent bank account located in New York.

A BEC victim in Colorado reported transferring $56,000 after receiving a spoofed email from a lending agent during a real estate transaction.

In both cases the FBI were able to freeze the criminals' accounts and the money was recovered. Others are not so lucky. In September 2019, an FBI public service announcement, **Business Email Compromise the $26 Billion Scam**, highlighted the magnitude of the BEC/EAC (email account compromise) problem. It stated that between May 2018 and July 2019 there was a 100 percent increase in what they refer to as identified global exposed losses.

INDUSTRY CASE STUDY: REAL ESTATE IS THE PERFECT TARGET FOR PHISHING

continued from previous page

THE ATTACKS ARE HIGHLY TARGETED

Because the return is so high, and so many phishing-as-a-service offerings facilitate attacks at low cost, the attacker can afford to spend time setting up the activity. There is plenty of information in the public domain that can be researched to lend authenticity to the attack – listing sites include details about houses that are for sale, the agent and, more importantly, the stage the sale is at, such as "under contract".

A number of phishing tactics are deployed to try and divert the payment, but most involve a fraudulent email requesting that payment be sent to the criminal's account. Who the recipient and spoofed sender are will be different in different countries and maybe states, depending on the property buying process.

Some attacks use simple impostor emails to spoof the sender, others will use the sender's real account. The latter clearly has far more chance of success, but is more complex as the account must first be compromised, typically using a credential phishing attack as the first stage. This provides far more benefits than simply being able to send an email from the compromised account. The attacker can spend days or even weeks hiding in the victim's email system, performing reconnaissance and gathering inside information that can then be used to construct the final email, to make it appear more authentic.

No email security can be 100% effective. BEC attacks are extremely difficult to detect and emails sent from compromised accounts impossible to detect using today's widely deployed secure email gateways. For this reason, your information security program should never focus on only technology controls. Information security is about technology, people and process controls. Preventing these BEC attacks is possible. Adopt processes that use out-of-band communications to verify money transfers and train people to enforce them.

Industries with complex supply chains are under attack

One trait of a business that often exposes it to increased risk is the complexity of its supply chain. Attackers will target the weakest link in the chain, often compromising a smaller, less well-protected company to use its trusted relationship with the real target to gain access to its network and systems. Many industries fit the profile, but especially logistics, transportation and manufacturing.

According to Forrester Consulting's research into the use of operational technologies and SCADA in manufacturing, more than 60% of the companies surveyed stated that they provide either "complete or high-level access to their SCADA / ICS" to other companies in their supply chain.

Logistics and transportation companies of all sizes also tend to have geographically wide-reaching and diverse supply chain connections, which significantly increase attack impact. The distribution of a single shipping container will likely involve information and goods transfer with at least ten different stakeholders, including the shipper, the consignee, a shipping line, origin and destination ports, a trucking company, and banks, as well as customs and border authorities.

Interaction between large and small companies in the logistics cycle contributes to the attack process. For example, in the high-profile Maersk attack of 2017, it wasn't only maritime ports and container vessels that were affected. Trucks destined for inland facilities were held up for hours and even days at various ports, waiting for the systems to come back online, so they could process and receive or deliver their shipments.

Phishing Sites Don't Last a Zero Day

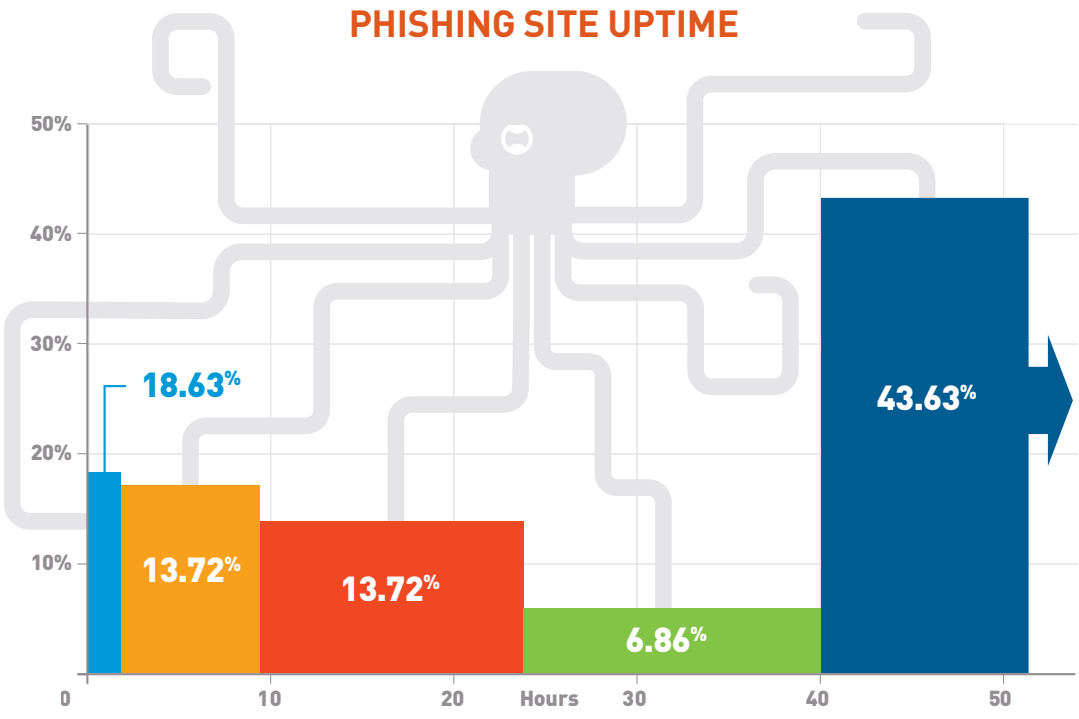
In an effort to better understand the complete phishing picture, Cyren experts examined phishing sites tracked and flagged by the Cyren's phishing intelligence data and analyzed how long these phishing sites remained online and active.

Because Cyren systems observe billions of internet transactions on a daily basis, our analysts often have a unique opportunity to do a deep dive into specific data sets, like quarterly phishing numbers. Using data from Cyren's phishing intelligence data, we analyzed how quickly website owners and their web hosting services responded to notifications that their sites had been hacked. Unfortunately, most hosting services pay very little attention to site hacking; site owners usually only become aware of a hack upon seeing a browser warning, or strange traffic numbers and destination sites in site analytics.

NOTABLY, THE HIGHLIGHTS OF CYREN'S FINDINGS INCLUDED:

- Nearly 20% of sites are gone within three hours.
- Half are gone within a day.
- Of the remaining 50%, over 40% stuck around for over two days.

While sites are still live, phishers resend email campaigns. Since greater than 50% of the sites examined remained useful for two days or more, clearly phishers are getting good mileage out of a hacked site. This also suggests that late protection still has some value for security providers, as the site may still be active; however, solutions offering full protection need to be prioritized and encouraged in order to block phishing sites during zero hour attacks.



What Companies Can Do to Improve Protection

With phishing increasing exponentially, companies need to think comprehensively about what they can be doing to protect and defend against phishing attacks.

PASSWORD MANAGEMENT

Password re-use makes phishing attractive for criminals. A breach into one system containing user names and passwords means that criminals will likely try to exploit the user names and passwords on other systems. Experts recommend a password manager that creates different and unique passwords for every site. Password managers also won't autofill information into a phishing site.

TWO-FACTOR AUTHENTICATION

By requiring employees to use a combination of two different components in order to log into a website, such as something an employee knows (a PIN or password) and something he possesses (a phone or token), the user's identity is more likely to be verified as legitimate.

PHISHING INTELLIGENCE

Ensure your cyber security includes real-time phishing intelligence that draws from large data sources and analytics and provides real-time protection from emerging web threats on all devices, including smart phones and tablets; immediate phishing threat notification; and continuous protection for all users.

USE DIFFERENT VENDORS FOR EMAIL AND WEB SECURITY

Information security best practice is to use multiple layers of security from different vendors. This allows for multiple attempts at detecting a threat by different technologies. If your email security fails to detect a phishing URL in an email and a user clicks it, your web security gives you a second chance at recognizing the site as malicious and blocking the user's connection to it.

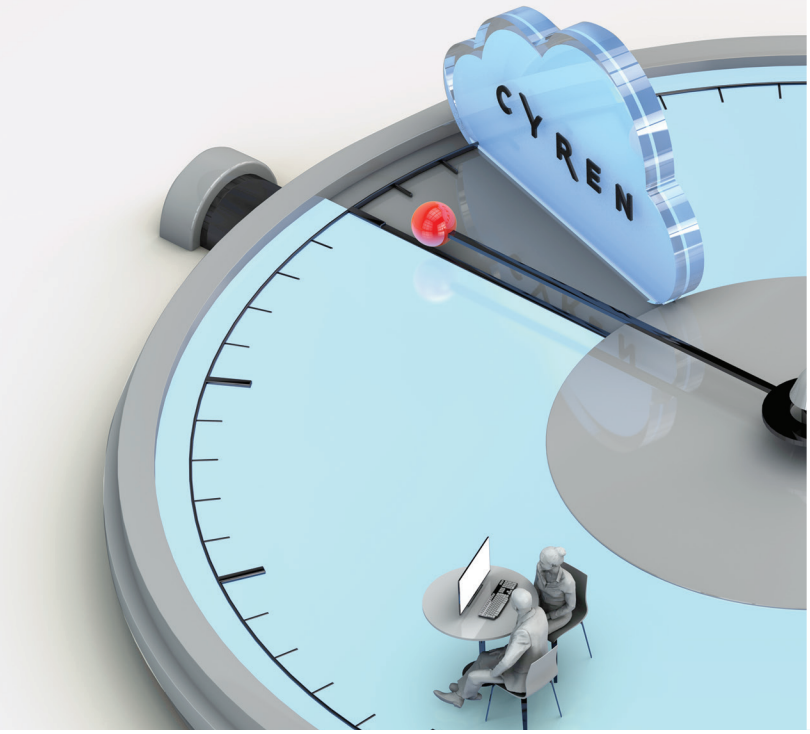
USER TRAINING

Educate and train employees on the dangers of phishing. Training options include everything from basic PowerPoints with phishing examples to simulated or "fake" phishing attacks. These will improve awareness for employees and ensure they don't become complacent. Consider including the cost and implications of a successful phishing attack in your training so employees know how serious these types of attacks are.

USER REPORTING

Most companies have a mechanism for users to report suspicious emails, typically to their IT team. New security solutions are emerging that include email client plug-ins that automate this process, engaging users at the point of risk and allowing them to perform an automatic on-demand scan of a suspicious email.

Cyren–The Fastest Time to Protection



The Appliance Window of Exposure

CYREN

Cyren is a messaging security company that protects enterprise email users from today's evasive threats and supplies threat intelligence solutions to security software integrators, hardware OEMs, and large service providers. Cyren's GlobalViewTM threat intelligence network analyzes billions of email and web transactions daily and is trusted by companies like Microsoft, Google and Check Point, who utilize Cyren's APIs and SDKs to operationalize threat intelligence for their customers.

Headquarters

US Virginia
1430 Spring Hill Road
Suite 330
McLean, Virginia 22102
Tel: 703-760-3320
Fax: 703-760-3321

Sales & Marketing

US Austin
10801-1 North Mopac Expressway
Suite 250
Austin, Texas 78759

UK Bracknell
Maxis 1
43 Western Road
Bracknell
Berkshire
RG12 1RT

US Silicon Valley
1230 Midas Way
Suite 110
Sunnyvale, CA 94085
Tel: 650-864-2000
Fax: 650-864-2002

R&D Labs

Germany
Hardenbergplatz 2
10623 Berlin
Tel: +49 (30) 52 00 56 - 0
Fax: +49 (30) 52 00 56 - 299

Iceland
Dalshraun 3
IS-220, Hafnarfjordur
Tel: +354-540-740

Israel
1 Sapir Rd. 5th Floor, Beit Ampa
P.O. Box 4014
Herzliya, 46140
Tel: +972-9-8636 888
Fax: +972-9-8948 214

Cyren.com

@CyrenInc

linkedin.com/company/cyren