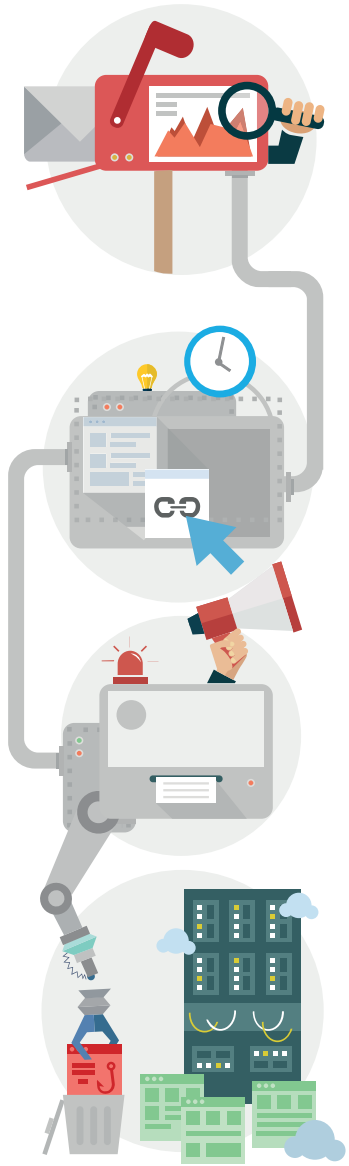
Vade Secure
Predictive Email Defense

Email Filtering for providers

How email service providers and ISPs can use anti-phishing, anti-ransomware and graymail filtering as a strategic weapon.

Win new customers, keep your current ones, and avoid being stuck in commodity pricing hell.

Table of Contents



Summary

Email Service Providers strive to deliver a great email user experience to retain customers and attract new prospects. This means engaging in a constant battle against unwanted email messages that range from mere nuisances to serious security threats. In response, a range of tools have come on the market that lower the risk-level and reduce the nuisance-factor for email users. As email-borne hacking grows more sophisticated and threatening, however, ISPs and hosts need new, more powerful tools that will help them address email threats simply and economically. This paper looks at new ways that ISPs and hosts can rise above the competition by tackling rising threats, such as spear phishing, while handling the age-old challenges of graymail and spam.

Introduction

Email is a bittersweet essential in the business of providing Internet service.

Your customers love email.
Email is critical. It is the most used internet-enabled service for virtually all of your customers. It is the linchpin of their professional and personal lives.

Your customers hate email.
Email is a massive hassle. It is filled with spam, dangerous phishing emails, malware and low-priority commercial communications (graymail). Plus, a growing number of highly sophisticated spear phishing attempts can cause massive financial and personal harm.

Email hassles cost you money, time and customers.
Dealing with email problems is a daily reality for ISPs and email hosts.

It's a cost center impacting:

- Technical support staff
- System administrator time
- Legal liabilities
- Lowered customer satisfaction and renewal rates

These costs are especially problematic in a sector that's all too often seen as a commodity. It's hard to raise pricing sufficiently to cover anything more than "standard" service. Attempts to staff up to address customer service issues are doomed because the avalanche of email problems grows exponentially while customers' willingness to pay does not. Users get increasingly frustrated as their legitimate problems get conflated with user ignorance.

The blame and cost for generic email problems land at the ISP's or email provider's door.

What is an ISP or Host To Do?

The answer lies in automated services that eliminate the hassles, pain, and support call requests in the first place. Happier customers do not need to be placated. Customers who were never exposed to an email threat do not require help recovering from it. Legal threats are not made form those suffering no damages.

Success comes to those who can rise above the rest of the pack and deliver a superior automated email user experience. Every ISP and email host provides email as a standard offering. As a consequence, if your email offering is "standard," then email becomes nothing more than a (substantial) cost of doing business. However, if your email offering is **exceptional**, it can become a critical differentiator, a massive competitive advantage and ***a generator of new business***.

> ***Exceptional email can be a strategic weapon with which you win new customers, keep current customers, and avoid being stuck in commodity pricing hell.***

This paper takes a look at the range of email threats and nuisances that present both a problem and an opportunity. The problems are all too well understood. The opportunity arises only when you can handle threats and nuisances better than your competitors. We delve into how you can bolster your email service by addressing the full collection of threats through an elegant, automated and unified solution.

The Spectrum of Email Threats and Nuisances

Providing an email service means dealing with a huge barrage of email messages that your customers don't want to see. While some of the rogue message forms are well-understood, new threat vectors and ever-more toxic versions of familiar threats appear every day.

Spam

More than half of all email messages in the world are spam. With our customers, we observe that at least 70% of inbound messages are spam. As of January, 2016, the percentage of Spam was up to 79%. Spam continues to evolve and evade filtering technologies. It's a good news/bad news situation. The good news is that spam can be contained, though the process is never static. Spam filters and malware detection software can be trained (and retrained) to detect and quarantine spam. Spam protection is never perfect, but there are several options available today that can efficiently block unwanted messages from the user's inbox.

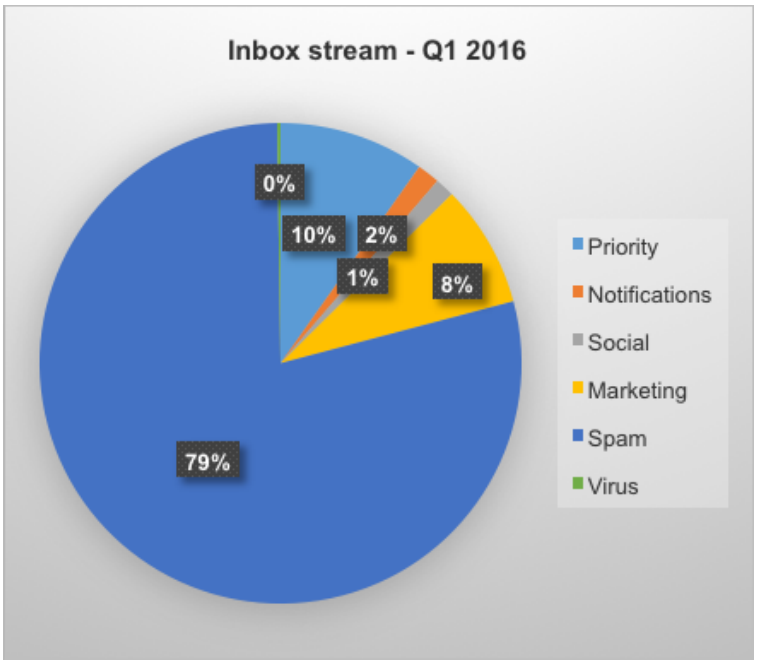


Figure 1: Email Statistics taken from 300 million mailboxes monitored by Vade Secure.

The bad news is that effective spam control is basically "table stakes." Your customers simply assume you can do it well. You're going to spend money and time on spam and still essentially be running in place, in competitive terms. Having good spam control won't get you new customers. Yet, if there's a problem, you're in trouble. If a tsunami of Cialis ads hit your customer accounts, your (expensively staffed) support line will start to ring.

Graymail

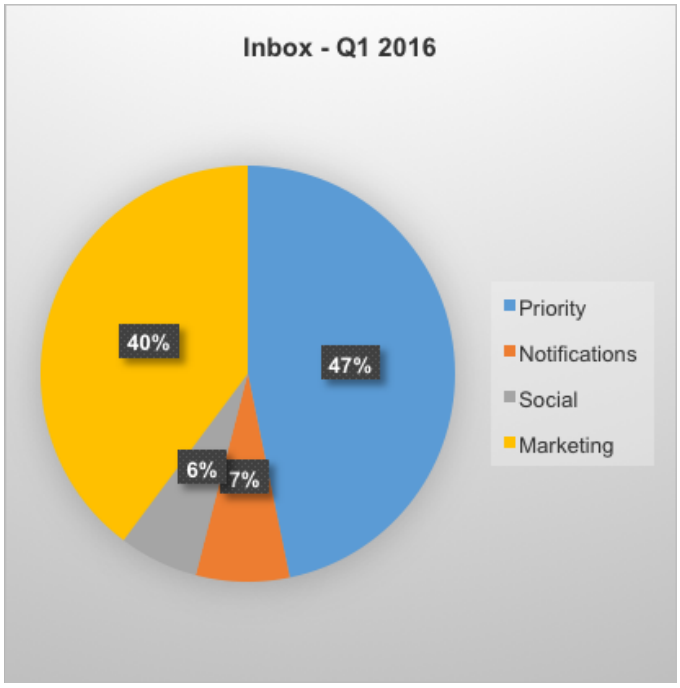


Figure 2: Detailed statistics of non-spam emails based on 300 million mailboxes monitored by Vade Secure.

The term “graymail” isn’t familiar to email consumers, but as an email provider or ISP, you likely know all about it. Graymail isn’t quite spam. The recipient did opt-in to receive it at some point. However, over time, the recipient has lost interest in the sender or even completely forgotten he/she ever agreed to get email from them. For instance, when a consumer is checking out at a retail store, the cashier asks for his/her email address. Later, the consumer starts to get sales pitches from a business he/she doesn’t remember. Graymail is often conflated with spam in a users mind… creating the perception of ineffective spam filtering. As **Gartner said,**[1] **“End users don’t care about the clinical definition of spam and are frustrated with the level of “unwanted” email in their inboxes.”**

With the right analytical approach, graymail can be filtered out of the inbox and reclassified as a commercial message or a social notification. Even better, tools can be provided to allow users to easily manage and opt-out of graymail with automated unsubscribe technologies. This presents an opportunity for competitive differentiation.

An analysis of millions of corporate email inboxes revealed that more than 50% of non-spam messages are graymail! This effectively hides priority emails from users. While graymail may on the surface seem like a mere nuisance, it significantly impacts productivity. When you help your customers’ employees be more productive, you will start to earn fans... and fewer support calls as well.

1 Magic Quadrant for Secure Email Gateways – July 2014

Phishing and Spear Phishing

Phishing is a different category of threat. Unlike spam, which is largely understood and contained, and graymail, which is merely perceived as a nuisance, Phishing and Spear Phishing are serious security threats. They're also increasing rapidly. Phishing attacks jumped up by 74% in the second quarter of 2015, for example.

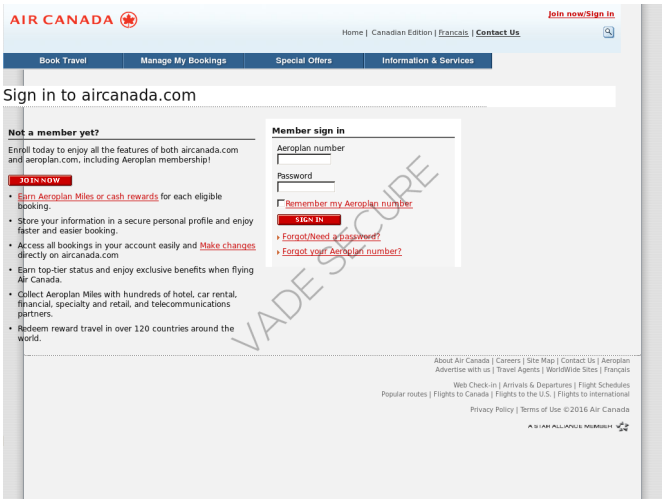


Figure 3 - A fake airline information web form. (Source: isitphishing.org)

Phishing attackers "fish" for victims by sending them deceptive emails. Virtually everyone has gotten such a message. Phishing emails request personal information under false pretenses or purport to offer the recipient prizes in exchange for entering personal information at websites that look real but aren't. Figure 3 shows a phisher's perfectly faked log in page from a major airline.

Spear phishing is the new variant on the basic phishing attack. It aims at specific employees of an organization with many goals, such as gaining unauthorized access to networks, data and applications or "simply" asking for an international wire transfer. In contrast to the rapid, mass email approach of phishing, which might see hundreds of thousands of attack messages go out within the space of a few hours, spear phishing is methodical, deliberate and narrowly focused. A typical spear phishing attacks will target a single company's accountant and can lead to a wire transfer of several hundred thousand euros or dollars.[2]

Phishing works. Twenty-three percent of recipients open phishing messages. Another **11% click on links** in phishing emails, according to security industry research.[3] The results can be devastating. **An estimated ninety-one percent of hacking attacks include a phishing attack.**[4] Some of the worst data breaches in the last few years are suspected to have originated with successful spear phishing attacks.

2 Fraud warning: increase in "Fake President" frauds, Deloitte.com.
3 Verizon 2015 Data Breaches Report
4 http://www.wired.com/2015/04/hacker-lexicon-spear-phishing/

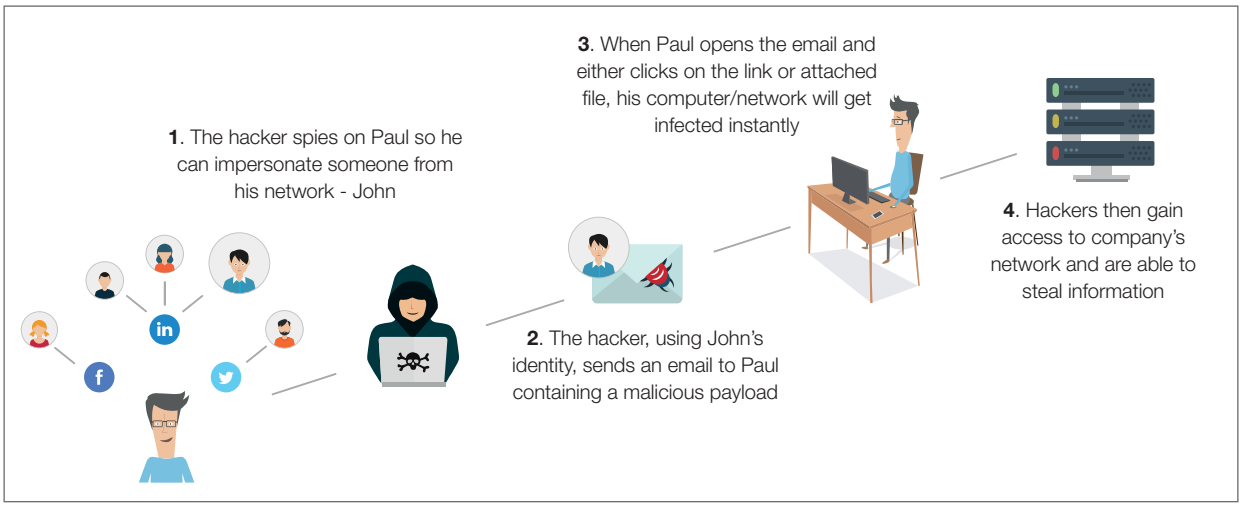


Figure 4 - The progression of a spear phishing attack, starting with research of the target organization and identification of a specific individual inside the organization, followed by a series of emails intended to build trust with the target.

How do spear phishing attackers get away with it? Successful spear phishing is based on establishing trust with the target. Consider the following example. Let's say you provide 500 email accounts to an insurance agency. A spear phisher wants to get inside the agency's record system in order to harvest personally identifying information about its clients.

The attacker's first step is to research the company's "about us" section to determine the target and start to create a cross-reference of social graphs. Using fake active Facebook and LinkedIn accounts and sometimes an active phone number, the hacker builds a list of who knows whom inside the company. The attacker identifies an insurance agent as a target and consult Yelp and similar online references to find the name of an insurance policyholder.

The attacker is now ready to send the target a series of emails, shown in Figure 4 that build rapport and trust progressively. The first message will be innocuous, like, "Hey, Joe. It's Bill. Are you going to the office party next week?" Once Bill responds, "Joe" escalates into asking about co-workers and policyholders. The messages become more like, "Bill. Joe here. Listen, can you tell me the date of birth for Sally Doe – I need to renew her auto policy." Finally, "Joe" sends a message that reads, "Bill, I'm in a jam here – out on vacation and away from my desk. What is the log in for the records database platform? I can't remember. Thanks!!! Joe."

Perhaps you're wondering, "How can 'Joe' fake being an employee of the agency. Doesn't he need a unique, domain-specific email through the agency? He should, but due to the agency's "Bring Your Own Device" (BYOD) policy, employees are able to use their own phones for work email. In this case, the attacker knows from LinkedIn that "Joe's" email address is joetheduckhunter@gmail.com. The attacker creates a Gmail account for joetheduck.hunter@gmail.com. Bill doesn't notice the difference, and the stage is set for the real attack.

Once Bill shares his log in, "Joe" can access the confidential files. As an alternative plan of attack, "Joe" could send Bill a document, such as an Excel file, which **contains key logging malware. Either way, the phisher can collect Bill's login credentials.** "Joe" can penetrate the networks and steal data. Bill may never even know that the attack has occurred.

Most spam filters and other standard email tools will catch the majority of untargeted mass phishing emails, but a few thousand messages almost always get through and they often are the most dangerous. It takes a short amount of time for filters to "notice" the pattern of a mass phishing email and block it. For those infected, it's too late.

Spam filters generally cannot catch spear phishing emails at all because they look like regular messages. They are targeted to a specific person and don't follow phishing email patterns. Each spear phishing email is unique. That is why they are very difficult to spot.

Malware through Phishing and Spear Phishing Campaigns

While phishing typically targets residential email users to ask for credentials, spear phishing emails target individual professional users to attack their companies. To do so, hackers have many options. One of their favorite and most dangerous is the malware injection. Often disguised as a Microsoft Office document (e.g., Word, Excel, PowerPoint) they are activated once the user opens the file and enables macros… Too late, the malware is on the device and may try to penetrate the company's network and even your hosting infrastructure.

There are several types of malware, each with different goals. The key logger mentioned above is designed to save the user's keystrokes. Ransomware encrypts everything it touches, from the server level to the device.

Malware injection through spear phishing is a critical problem for email users. It's currently the most dangerous threat.

Stopping Spear Phishing is Difficult

Spear phishing emails are essentially invisible to standard spam filters. Spam filters look for URLs, topics and keywords that signal that something isn't right about the message. The filters is trained to look for phrases like "Get Cialis for 99 Cents!" Even a good spam filter won't notice "Hey, Joe. It's Bill. Give me a call." There's no URL in the message that could get flagged. There's no file attachment. There's no suspicious keyword. The message breezes through to the inbox. Money or IP is stolen. Awareness of the threat that spear phishing represents grows.

There's an opportunity here, as awareness of spear phishing increases, an enterprising ISP or email host can differentiate itself by offering a solution. It's compelling because spear phishing is far more than an email security threat. It's a very serious risk factor overall. The spear phishing email is simply the point of entry into the network. From there, the hacker can wreak havoc on the enterprise. Think Sony Pictures, Anthem Blue Cross, the US Office of Personnel Management and on and on… these are all thought to be the work of spear phishing attacks.

> ***If you can heroically protect your customers from this onslaught, not only can you use it as a compelling sales pitch, you can charge a premium for it too.***

Hard Costs of Email Threats and Nuisances

It costs money to give customers a good email user experience.

Obvious costs include software licenses, infrastructure and administrative time to oversee the anti-spam and anti-phishing systems. You also see the costs of managing email threats in customer service and technical support budgets.

Massive costs can also roar into existence when a customer suffers a serious security incident due to email based hacking. The damages to your client from a big data breach can easily reach tens of millions of dollars. Yes, user agreements and other covenants can shield you from liability, but they can't protect you from

the expense of dealing with the trouble. You can still get sued even if you're legally shielded. You'll spend a lot of time and money explaining how you're shielded and you could still lose or end up settling as a way to avoid paying excessive legal fees. And, of course, you can still lose customers and suffer devastating PR blows and reputational damage.

Opportunity Costs of Email Security

The biggest costs for lackluster email are opportunity costs: lost sales, customer churn, and being forced into commodity pricing.

> ***Spectacular email represents a massive opportunity: new sales, higher renewal rates, and differentiated pricing power.***

People want good email. It's the #1 business and personal communications tool. For instance, Gartner revealed that that 96% of email users want better protection against phishing attacks.[5] If you can deliver, you can play to the overwhelming segment of the market that is demanding this kind of security enhancement.

Mitigating the Full Spectrum of Email Threats

Vade Secure offers ISPs and email providers a competitive edge through a single suite of tools that mitigates the full range of email threats and costly nuisances. These include solutions for graymail, spam and phishing. Together, they form a comprehensive solution for managing risks in email and delivering the kind of user experience that keeps email customers loyal. As a single vendor solution, it is more cost effective to acquire, deploy and operate than a heterogeneous collection of solutions.

5 Gartner - Magic Quadrant for Secure Email Gateways – June 2015

Heuristic Filtering and Rules to Fight Graymail and Spam

ISPs and email hosts can leverage Vade Secure's comprehensive, behavioral system to filter email and assign messages to the inbox, spam or graymail folders. A global filtering engine, Vade Secure uses predictive heuristic filters, pattern recognition technology and a reputation management system to filter messages with a proven 99.99% accuracy. What's more, exclusive heuristic technology makes Vade Secure efficient from the first email of an attack wave, with high "zero-day" responsiveness, even on low-volume email waves.

The filtering technology works off of thousands of rules, each of which contributes to a fully independent evaluation of each message. There is no need for the system to learn anything specific about the deployment site or query an external reference server. In addition to being able to detect Spam and malware the system can classify commercial email, social networks notifications and newsletters as graymail. The engine is able to differentiate graymail from a booking confirmation from the same sender.

Figure 5 depicts the analysis-to-classification process in action.

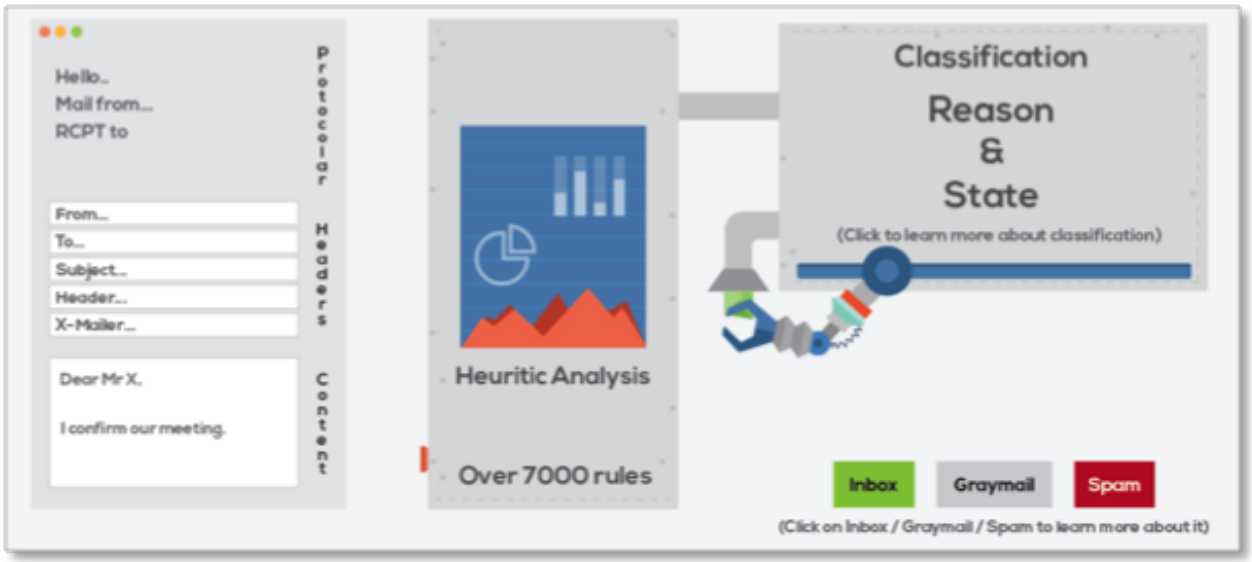


Figure 5 – the Vade Secure filtering process, using heuristic analysis to classify emails and assign messages to inbox, graymail or Spam.

Anti-Phishing/Spear Phishing

Vade Secure's anti-phishing solution is focused on the specific problem of phishing, including specific features such as looking at credential requests and Identity Match™ that are tailored to fighting spear-phishing attacks. It can be layered on top of existing anti-spam solutions – Vade Secure or others - to provide better overall email protection to your customers. Our comprehensive solution includes:

- *Content email filtering.* This artificial intelligence has been trained by monitoring hundreds of millions of email boxes for 10 years looking for phishing threats. It heuristically evaluates email content, requests for credentials, phone numbers, DNS (URL) reputation, any linked website content and much more. Unlike other pattern-recognition technologies, our filter looks at the characteristic of each email and is therefore much more reliable for low-volume email scams and spear phishing attempts. It can catch the first phishing email that comes into your organization…even if there is only one.

- *Webpage exploration at the Time-of-Click.* Every URL that is included in any email is safely explored in a remote sandboxed environment to see if it contains any malware or other malicious code. What makes our solution unique and superior to other tools is that this exploration is done at the time an employee clicks on it. Competing solutions examine URLs at the time the email is received by the network. This is important because sophisticated hackers will now send emails that include URLs that initially lead to innocent websites, then wait to redirect those URLs an hour or two later, thus bypassing most filtering systems unless the site is examined at the time of click.

- *Identity Match™ advanced spoofing detection.* This patented set of spoofing protections identifies every incoming email that attempts to spoof trusted company domain names, display names and even similar but different email addresses that are close to real ones. Identity Match looks at both technical and style indicators of every email and compares them to previous communication habits. The solution identifies similarities between new senders and all your previous contacts in order to identify if there is a spoofing attempt targeting your company. This unique feature helps to identify and isolate even highly sophisticated one-off spear-phishing attempts.

- *Education and remediation.* Vade Secure provides educational banners to users who receive phishing emails informing them of the threat posed and how they can avoid it. These impossible to ignore integrated banners alert users to the possibility of a phishing attempt right in the message itself. We also alert administrators if users have ignored phishing warnings on either email links or URLs and have thereby potentially created a breach of security.

Anti-Malware and Attachment Analysis

Over the past few years, major malware have been increasingly hidden in common files such as PDFs and Microsoft Word documents. This avoids security filters that only examine and block executable files (.exe). Vade Secure Outbreak has a specific technology focusing on Office documents in which Vade Secure analyzes the behavior of the embedded macro code. In addition to the analysis of the malicious code, Vade Secure identifies whether the document will attempt to get malicious code from outside.

All attachments are thoroughly investigated in a remote sandboxed environment to eliminate possible malware. The attachments are analyzed, taking into account the environment where they originate. Vade Secure's unique attachment analysis algorithm examines the proprieties of both emails and attachments. This gives Vade Secure the ability to predict the advent of a "0-day" attack from previously unknown vectors. It is also possible to add anti-virus add-ons such as Dr. Web.

Phishing Webpage Takedown and Host Alert

To secure the web on several layers, Vade Secure provides tools that help hosting companies clean their infrastructure. We developed a cPanel plugin dedicated to hosting companies that scans webpages to detect elements used in phishing. The malicious pages can be set for either manual or automatic deletion.

We are also able to alert you in real time when we have detected a phishing webpage on your servers.

Solution, Deployment, and Reselling Options

Choose from either a complete suite of email protection or specific point solutions that layer over your current email systems:

- Anti-Phishing/Spear Phishing
- Anti-Spam
- Anti-Malware
- Graymail Management

Deployment options include:

- Hosted/SaaS
- Gateway/On-site
- Plugin for C-panel
- Plugin for Zimbra and integrated in most common webmails
- Software Development Kits to integrate Vade Secure's email security with other applications.

Vade Secure is extremely friendly to white labeling, resellers, and OEMs. Our solution is highly customizable, multi-tenant enabled, and can seamlessly integrate into your existing offering.

Give us a call at 415-745-3630 if you want to discuss how you can quickly start offering email security that differentiates you from the competition.

About Vade Secure

Vade Secure is the global leader on anti phishing, spear phishing, malware and ransomware filtering. Language independent, the filter analyzes globally all incoming emails (links, attached files, content…) to detect all threats in zero-day, even the most targeted attacks. After elimination all threats, we eliminate the nuisance of low priority emails with the Graymail Management. Ads, social networks notification and newsletters are automatically sent to the graymail folder while the Safe Unsubscribe button eliminate them forever.

Protecting more than 400 million of mailboxes in 76 countries, our solutions are used by major ISPs, OEM and Enterprises worldwide. Vade Secure is implanted in 5 countries (USA, Canada, France, Hong Kong and Japan) to offer a 24/7 support.