



## GET MORE INFO

[rpinfo@returnpath.net](mailto:rpinfo@returnpath.net)

1-866-362-4577

## The Anti-Phishing/Anti-Spoofing Guide: What Every Email Marketer Should Know About Brand Protection and Securing the Email Channel

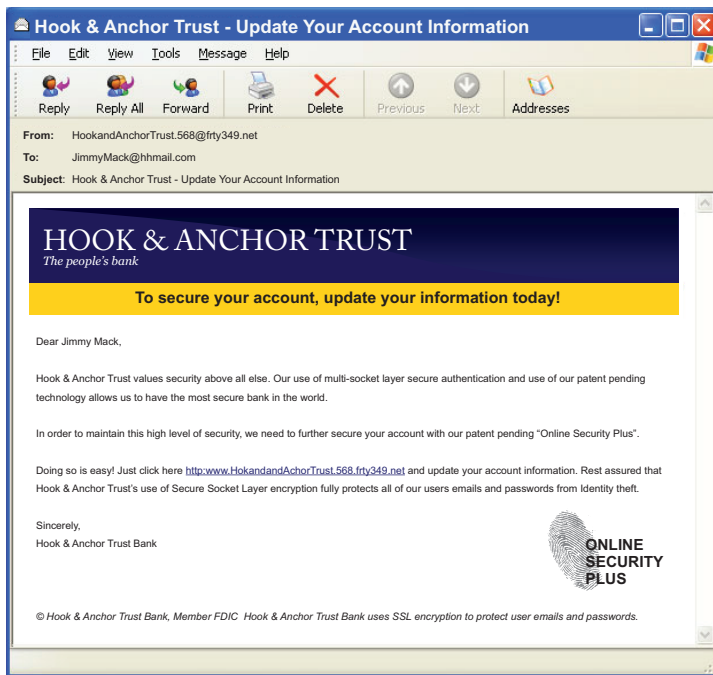
### Organized gangs victimize millions—including hundreds of email marketers!

Sensationalist? Yes. Unfortunately, it is also true. Last year more than 200,000 malicious phishing attacks, involving billions of emails, were perpetrated, most by organized phishing gangs.<sup>1</sup> The phishers stole individual account numbers, took over computers and even took control of whole computer networks.

It's ugly—and so is the impact on the brands that are used in the phishing attacks. Each month about 250 brands are affected, including trusted brands in every vertical —social networking, e-commerce, retail, consumer goods, travel, insurance, online games and others. Gartner estimates that phishing attacks cost organizations \$3.6 billion/year, and that is just the direct cost of repairing the damage.

For email marketers, having your brand used in a phishing attack is a disaster. Much of the investment you have put into building trust and developing customer relationships is suddenly useless. Current and prospective customers lose trust in the brand, and become reluctant to do business with the brand online. Return on marketing investment decreases.

This paper provides background on phishing and spoofing, discusses current approaches to managing the risks, and highlights a new and more effective way for companies to protect their domains and brands, and guard against the cost of fraud.



## A PHISHING STORY

The email from the bank looked authentic enough. Under the company logo, it opened with a long, well-written explanation of the importance that the bank placed on protecting personal data. The message went on to explain that in order to maintain security, the customer needed to secure his account with “Online Security Plus” and update his account information. It closed with the reassurance that the bank used Secure Socket Layer encryption to protect user emails and passwords.

Anxious to be sure his online bank account was secure, the customer clicked through to the bank’s website and completed the form, providing his name, credit card account number, social security number, security word, email address and password. Unfortunately, it was not the bank’s website, but a well-crafted forgery. Within a day, he was a victim of identity theft. It took

months for the customer to close all of his affected accounts, fight the damage to his credit report, and open new accounts. Two years later he still had to monitor all of his accounts closely. He had unsubscribed from bank email and no longer did any banking online.

This customer had a miserable experience—and so did his bank. They had to help hundreds of customers in the same situation, and absorb financial losses. Yet the bank had done nothing to cause that experience. Both customer and bank were the victims of a “phishing” attack.

Today trusted brands in every vertical – social networking, e-commerce, retail, travel, consumer goods, online gaming, insurance, etc. – have become victims of phishing attacks. In fact, fraud in the form of phishing and spoofing impacts not only its immediate victims, but also the organizations whose well-established brands it abuses.

- Every day more than 260 million fraudulent emails, pretending to be from a trusted company, are sent to consumers.
- In the second half of 2009, there were at least 126,000 phishing attacks, more than double the number recorded in the first half of the year<sup>ii</sup> and in 2010 there were 203,000 attacks.<sup>iii</sup>
- 42% of respondents in a Cloudmark Survey felt that their trust in a brand would be greatly reduced if they received a phishing email claiming to be sent by that brand.<sup>iv</sup>

Gartner estimates that phishing attacks cost organizations \$3.6 billion per year, but those are only the “hard dollar” costs to repair the damage.

When your company’s brand is used in a phishing attack, the costs to your trusted brand, to your company’s reputation and to consumer trust in the email channel can be even more significant. According to the 2010 Identity Theft Resource Center survey, 81% of consumer respondents cited phishing emails as a significant concern relating to the security of their personal and financial information when conducting online transactions, indicating just how significant the impact on trust can be.

## GO PHISH: HOW IT'S DONE

In the more commonly known form of phishing the phishers attempt to get someone to voluntarily surrender their password or other Personally Identifiable Information (PII) by fooling them into believing that they are interacting with a legitimate website. This is usually done by sending an email message that contains links to a forged website—a site that looks like it belongs to a legitimate brand, but does not. These emails often include messages with a sense of urgency about the need for the recipient to provide information in order to correct a problem. When users provide the requested information (e.g. account numbers, passwords, and social security numbers) the phishers typically sell them to identity thieves.

Sometimes phishers use web addresses that are very close to the names of well-known companies, but with a minor alteration that many people would miss, for example [www.microsoft.com](http://www.microsoft.com). They frequently use compromised servers that they have hacked into—but not those of the brand they are spoofing.

## MALWARE ATTACKS

The less commonly known form of phishing is even more problematic: the malware attack. These attacks are becoming more common. In a malware attack, the victim is induced to click on a link to what appears to be a legitimately branded website. Once the link is clicked, some form of malware (malicious software) is downloaded onto the victim's computer. Since the victim does not have to do anything at the forged website to be victimized, malware attacks may go unnoticed for extended periods.

Phishers take advantage of this extended time, using downloaded keyloggers to steal passwords to all the victims' online accounts, adding the computer to a "botnet" that can be used to send out further phishing emails, or exploiting a security flaw on the computer to control it remotely and conduct online transactions. While "traditional" phishing provides a phisher with a single credential or single set of credentials that are valid for a short period, malware-based attacks allow ongoing access to both the user's computer, and any network resource the user can access.

Malware attacks can also be combined with phishing attacks. In this form of attack, the victim visits the compromised site, falling prey to a drive-by malware download, and the site also attempts to collect login credentials. If someone provides private information on a site like this, they have been duped twice.

## THE NUMBERS GAME

Phishers know that only a tiny percentage of people will respond to their emails, so they play a volume game to assure they will get thousands of victims. Worldwide, it is estimated that 8.5 billion phishing emails were sent every month in 2008.<sup>v</sup> According to Gartner, there were 3.2 million victims of phishing scams in 2007, with an associated average dollar loss of \$886 per victim.<sup>vi</sup> More than 29,000 phishing websites were operational at the end of March 2010, according to the Anti-Phishing Working Group, and the number has gone as high as 56,000 in the past.<sup>vii</sup>

While many computer users are now able to identify the most traditional forms of phishing emails, phishing gangs have become more sophisticated in the emails that they send, making it a real challenge for recipients to identify every phishing email. SonicWALL found that only 7% of the people completing its phishing quiz were able to correctly classify all of the emails on the quiz as phishing or legitimate email.<sup>ix</sup>

**A single syndicate employing advanced malware was responsible for two-thirds of all the phishing attacks detected in the second half of 2009.<sup>viii</sup>**

## FORGING A PATH

'Spoofing' refers specifically to the technique of making an email message appear to be from someone else through forging of the From, Return-Path, and/or Reply-To headers. It's unfortunately easy to do this, because the email system was not designed with built-in protections against this sort of thing. Phishing emails are usually sent with spoofed "From" addresses and make use of brand graphics so that the email looks like it comes from the company it purports to be from.

## SPEARS AND WHALES

Spear phishing is phishing targeted at employees or members of a specific organization or online group. Phishers may pretend to be someone that the organization or company has some relationship with, or they may dangle other extremely targeted bait. The phishers may use information that is publicly available through search engines or on websites like Facebook, MySpace and more recently, LinkedIn, to create emails that convince some members of their target population to go to a login page. The goal may be to get inside a company or organization's network. Once inside, additional attacks such as data exfiltration will take place.

**76% of organizations learn of an attack from their customers.<sup>x</sup>**

"Whaling" is phishing that is targeted at corporate executives, affluent people and other "big phish." Like spear phishing, whaling emails often are customized with information directed to the recipient (name and other personal information) and sent to a relatively small group of people. In one example, thousands of corporate executives were apparently served with subpoenas from the U.S. District Court in San Diego. The victims, convinced by the image of the official seal from the court, clicked on the link to download a copy of the entire subpoena. Unfortunately, when they clicked they had keylogging software installed on their computer.

## THE COST TO YOUR BRAND

If your brand is used in a phishing scheme, your company is the largest victim. You have invested heavily, probably over many years, into establishing a brand that people trust—and a brand they will do business with online. When that brand is used to defraud people, that trust is badly damaged, even though your company was not responsible.

The brand will inevitably suffer from reduced return on investment for its marketing expenditures. Victims, most of whom are not familiar with how phishing works, may feel that if the company had proper security, this would not have happened. Customers may be non-responsive to future email marketing, unsubscribe from email lists, or completely move away from your brand. The potential magnitude of impact can be significant; the lifetime value of a customer who uses email can be as much as 80% higher than a customer who does not. The "soft" costs of rebuilding trust in your brand can be tremendous.

If you think that your brand is not of interest to phishers, think again. Right now, 25% of the brands used in phishing are outside the financial and payment services industries. This portion is likely to grow as malware attacks become increasingly more common. With malware, no company is safe. Any respected brand can be used to lure people into clicking through to a fraudulent website if the goal is to get malware onto their computers. Recently publicized attacks have included LinkedIn, Hallmark, UPS, Amazon, eBay and even Coca-Cola.

## PHISHING: THE COST OF REPAIRS

When your brand is phished, your company will need to repair much of the damage, even though it had nothing to do with perpetuating the fraud. Once a company learns about the scheme, the scheme has usually been in operation for some time.



The company then has to expend staff time to:

- Research which accounts or customers were compromised
- Handle a spike in customer service calls
- Absorb costs from fraudulent transactions
- Reach out to those affected
- Issue new credit cards and possibly passwords, as required
- Work with and provide information to law enforcement/government agencies
- Provide customer education on phishing and identity theft

Executives may also need to invest time in handling unwanted media exposure.

In a conventional phishing scheme, the victimized brand may have to absorb hard dollar costs including fraudulent credit card charges and cash withdrawals from compromised accounts. There will also be costs for “takedown services”, which assure that fraudulent websites are taken down (see side bar).

## PROTECTING YOUR BRAND

Prevention is clearly the best approach to phishing. One key to protecting your brand is to educate your customers. Tell them how phishing works, and be very specific that your company will never seek to resolve account problems online. Let them know that they should send any phishing emails they receive to spam@uce.gov, to the organization being impersonated, and to reportphishing@antiphishing.org.

## DAMAGE CONTROL

For phishers, the first hour of any attack is the most productive. Fifty percent of all credentials are stolen in the initial hour of a phishing email campaign. One industry study refers to this as the “golden hour.” Within five hours, more than 80 percent of credentials are stolen, and the first ten hours yield more than 90 percent of all credentials that the phishers will get from that forged website.<sup>xi</sup>

Given this time frame, it follows that rapid take down of phishing websites is crucial to damage control. Rapid take down requires awareness. When the brand owner is aware of the phishing site and involved in takedown efforts, the average uptime for phishing websites hosted on compromised machines and free web hosting services drops from about 50 hours to about 4 hours.<sup>xii</sup>

### BEST PRACTICES TO PROTECT YOUR BRAND FROM PHISHING ATTACKS

- **Educate:** Educate your subscribers on how to identify a legitimate email from you. Highlight any unique features. Tell them you never ask for account information in an email. Communicate the look and feel of your email program to your subscribers and give them tips on recognizing a forgery.

Employees also need to be educated on phishing and how to respond if they find your brand is under attack.

- **Follow Email Marketing Best Practices:** Phishing messages often have poor grammar, misspellings and weak HTML coding. By following best practices for both email response and deliverability, not only will you increase the chance that your messages will reach the inbox, but your customers will more easily be able to differentiate between your messages and those of a spoofer.
- **Authenticate:** Authenticating all your email with DKIM and SPF is the only way to validate your sending identity and assure ISPs that they can block non-authenticated mail.
- **Inventory:** Take inventory of all your domains, including those that are “parked” (domains from which you never mail).
- **Prepare:** Have a plan in place to handle phishing messages that spoof your domain. This may include:
  - » Establishing a “rapid response team” with clearly delineated responsibilities for handling the aftermath of an attack
  - » Creating boilerplate external and internal communications to customers and employees that can be quickly tailored to the specifics of the attack and distributed.
  - » Take Down: Work with a takedown vendor to assure that all phishing sites related to the attack are dismantled.
  - » Respond: Notify your customers that your brand is being phished and what to look out for. Notify local and federal authorities (or applicable legal organization) of the crime.
  - » Join a Registry: Joining a trusted sender registry allows ISPs to block unauthenticated messages that use your domain (see below).

## REACTIVE PROTECTION

There are security tools and services to control and eliminate phishing attacks once they have been launched.

- Takedown providers work with domain registrars to take known phishing sites offline, replacing a fraudulent website with a “page not found”.
- Anti-phishing vendors monitor data / spam feeds from ISPs, email providers, anti-virus vendors partners and honey pots to help detect attacks (although this data is not necessarily comprehensive) and send URL feeds to known security vendors such as Symantec and McAfee, URL blacklists, etc. so they can use this information to block the site when a user clicks on a phishing link.
- Brand protection vendors monitor domain registrations and the WHOIS database for suspicious names and illicit activity.

Unfortunately, all of these services are reactive, rather than preventive. By the time they are engaged, most of the damage to the brand will already have been done.

Spam filters can help catch a lot of phishing spam through analysis of what a typical phishing email looks like, but just as with regular spam, much will slip through. Phishing gangs are making it more difficult for automated systems such as spam filters to detect the presence of red flag keywords (such as “PayPal” and “credit card”) by replacing those phrases with images that look like text.<sup>xiii</sup>

Some websites have implemented authentication mechanisms like “personal security images” and phrases that convey familiarity, uniqueness, and validate the site to the customer.

## AUTHENTICATION: NECESSARY, NOT SUFFICIENT

Authentication verifies the identity of an email sender, either by matching a sending IP address to the domain (for the SPF--Sender Policy Framework--and Sender ID version of authentication) or through public key encryption (for the DKIM--DomainKeys Identified Mail version of authentication). The SPF and Sender ID approach require that the sender publish text records in the Domain Name System for every domain from which it sends email. DKIM signs each message in a way that is difficult to spoof.

Authentication is an excellent mechanism for assuring an ISP that an email is from the apparent sender, but absence of authentication doesn't necessarily mean that an email is not legitimate. In theory, ISPs should be able to block phishing emails at the gateway because they are not authenticated. But because too many legitimate senders are not signing (authenticating) their email or doing it incorrectly, ISPs are afraid to simply block non-authenticated mail.

A brand owner can block any email that is spoofing their domain if they enter into an agreement with individual ISPs. Currently Gmail and Yahoo! do this with some senders, namely eBay and PayPal. This is effective for a limited number of brands like these, which are among the most spoofed in the world, but it doesn't scale. ISPs don't have the staff or time to negotiate individual agreements with every legitimate sender out there. What the ISPs need is a registry of senders who can affirmatively assure the ISP that all of their mail is being authenticated.

## THE SOLUTION: TRUSTED SENDER REGISTRIES

Trusted sender registries are a way of bringing together senders who want to protect the integrity of their brands and mailbox providers who want to protect their customers from potentially harmful emails. Senders in registry programs can protect the integrity of their email and web domains, guard against the cost of fraud, protect their email channel, and

communicate their signing practices to participating ISPs in one central place. Mailbox providers can know with certainty which domains are signing all of their outbound mail, so they can block unauthenticated mail at the gateway, protecting their customers from phishing and fraud.

To participate in the program, senders must publish their Sender Policy Framework and sign all outbound mail with DKIM. Mailbox providers must check SPF and DKIM on inbound mail.

Here is how Return Path’s trusted sender registry, Domain Assurance, works:

1. Senders in the Domain Assurance program add their domains to the Domain Assurance Audit List.
2. Participating ISPs send Return Path authentication results data for all domains on the Audit List, as well as copies of messages that fail authentication for these domains
3. Senders on the Audit List use Return Path’s Domain Assurance Dashboard to inspect reported data. They are able to view all email streams coming from a domain, validate their own authentication practices and identify authentication problems that need to be fixed.
4. In addition, they can use the data to identify fraudulent emails, phishing URLs and to engage their takedown vendor.
5. Once the sender is confident that all their email is indeed being authenticated, they can place their domains and sub-domains on the Domain Assurance Registry, asking ISPs to reject all mail coming from these registered domains that fails SPF and DKIM.

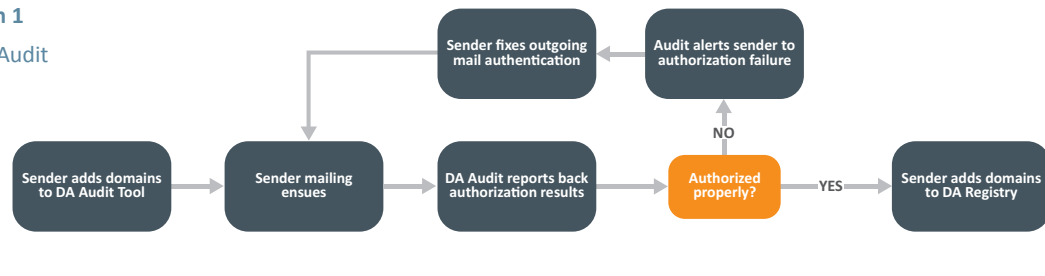
Senders on the Registry continue to receive data reports just as if their domains were on the Audit List, providing them with:

- Alerts when fraudulent emails using their domains are observed.
- Email intelligence on attackers and phishing URLs.
- URLs of malicious websites so they can initiate the take down of fraudulent websites (there may be hundreds of URLs being used per domain).<sup>xiv</sup>

The email coming from brands authenticated by the Domain Assurance Registry will have a Trustmark next to it within the inbox and/or within the message itself, at some participating ISPs.

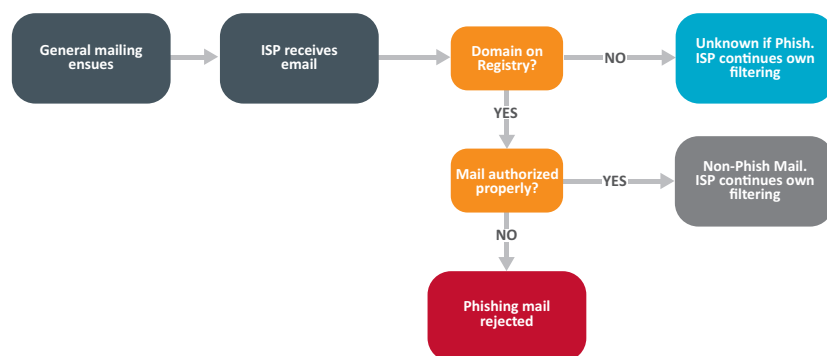
**Diagram 1**

Sender Audit



**Diagram 2**

After adding domains to Domain Assurance Registry



Trusted sender registries like Domain Assurance are complementary to takedown services. By using both together, your organization can prevent the business distraction of responding to a phishing attack, and prevent the significant hard dollar costs of an attack. Even more important, you can safeguard your brand equity and retain trust in your email marketing channel.

## ABOUT RETURN PATH

Return Path makes email work better. We certify email senders from around the world. Our trusted sender registry protects brands and retains trust in the email channel. We help marketers, publishers and other large-volume email senders increase their response rates by providing the world's leading inbox deliverability solution. Return Path helps mailbox providers and email administrators at ISPs and enterprises block unwelcome and malicious email by providing near real-time IP reputation scores and other data-driven tools.

Taken as a whole, these tools and services improve the consumer experience of email by protecting them from spam, phishing and other abuse. Return Path offers free access to Sender Score, the email reputation measure compiled through our cooperative data network of ISPs and other email receivers, at our reputation portal: [www.senderscore.org](http://www.senderscore.org).

Information about Return Path can be found at [www.returnpath.net](http://www.returnpath.net).

## ABOUT DOMAIN ASSURANCE

Return Path's Domain Assurance solution protects brands against fraudulent email activity and puts trust back in the email channel by blocking malicious emails purporting to be from your company at the gateway of ISPs and mailbox providers before they ever reach your customers. A unique anti-spoofing and anti-phishing service, Domain Assurance protects brands from phishing attacks and assures the continued integrity of their email channels. Through our unique data sharing relationship with hundreds of ISPs and mailbox providers around the world, Return Path provides senders with the broadest set of email data in the industry to detect attacks that no one else can find.

<sup>i</sup> "Phishing Attacks Increase 27% in 2010," RSA Monthly Online Fraud Report, January 2011

<sup>ii</sup> AntiPhishing WorkGroup, Global Phishing Survey: Trends and Domain Name Use in 2H2009; [http://apwg.org/reports/APWG\\_GlobalPhishingSurvey\\_2H2009.pdf](http://apwg.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf)

<sup>iii</sup> "Phishing Attacks Increase 27% in 2010," RSA Monthly Online Fraud Report, January 2011

<sup>iv</sup> Cloudmark, <http://www.cloudmark.com/en/article/reputation-of-uk-brands-dramatically-affected-by-phishing-attacks-according-to-survey-commissioned-by-cloudmark>

<sup>v</sup> SonicWALL, <http://www.sonicwall.com/phishing>

<sup>vi</sup> Gartner, December 17, 2007

<sup>vii</sup> AntiPhishing WorkGroup Report, Q1 2010

<sup>viii</sup> *ibid*

<sup>ix</sup> SonicWALL, <http://www.sonicwall.com/phishing>

<sup>x</sup> The Faces of Fraud: Fighting Back, Executive Summary, iSMG Information Security Media Group, December, 2010.

<sup>xi</sup> "The Golden Hour of Phishing Attacks," <http://trusteer.com/blog/golden-hour-phishing-attacks>

<sup>xii</sup> "The Impact of Incentives on Notice and Take-down" Tyler Moore and Richard Clayton, Seventh Workshop on the Economics of Information Security (WEIS 2008), June 25–28 2008.

<sup>xiii</sup> Netcraft, [http://news.netcraft.com/archives/2005/05/12/fraudsters\\_seek\\_to\\_make\\_phishing\\_sites\\_undetectable\\_by\\_content\\_filters.html](http://news.netcraft.com/archives/2005/05/12/fraudsters_seek_to_make_phishing_sites_undetectable_by_content_filters.html)

<sup>xiv</sup> AntiPhishing WorkGroup Report, Q1 2010

