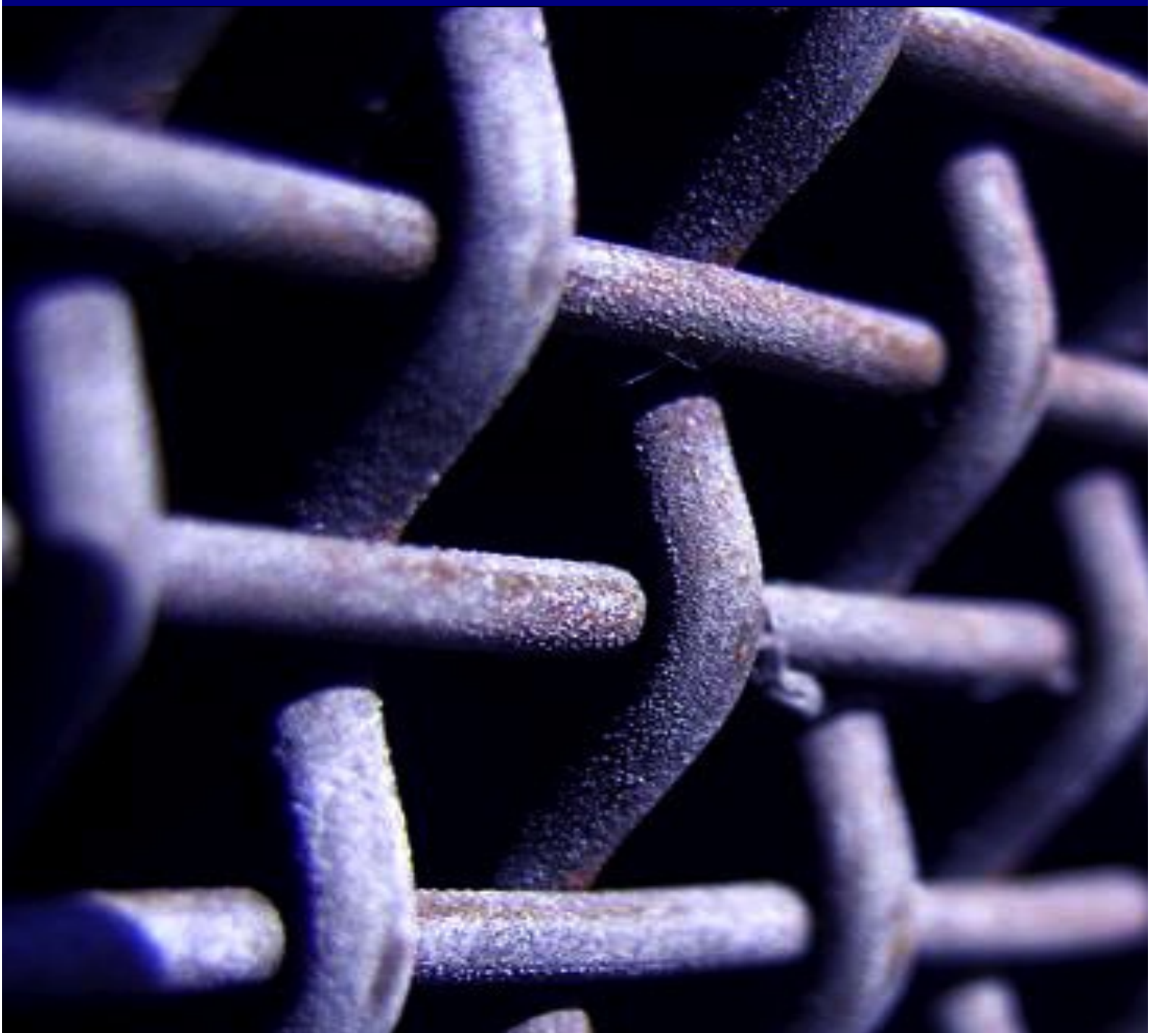
White Paper

The Phishing Crisis:
What it is, Why it Matters and What You Can Do

MALCOVERY SECURITY



Disclaimers

The information contained in this document is subject to change without notice.

The information in this document is provided for informational purposes only. Malcovery Security specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.

Table of Contents

What Is Phishing, Really?

Phishing attacks continue to threaten brands and their customers across the globe. According to a recent infographic produced by via resource, 37.3 million users were subject to phishing attacks in 2012.

As consumers increase the amount of time that they spend online, cybercriminals are ramping up their productivity – launching larger, more efficient and increasingly targeted attacks against brands both in and outside the financial services industry.

But, what precisely is phishing?

At Malcovery, we deliver email-based anti-phishing solutions. Through our interactions with prospects and customers, we've realized that there are several definitions of phishing floating around and that often the term "phishing" is used interchangeably with terms like "malware" and "spam."

What's in a word? Well, it's an important distinction. While phishing, malware and spam are rampant in today's threatscape, they are not one and the same. Pure phishing threats are analyzed and acted upon differently than spam and malware.

A general definition of phishing by Wikipedia:

"Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication."

Phishing is admittedly a wide-reaching term. There are several ways to carry out a phishing attack, which is likely why some of the confusion comes into play. In the broad sense, you could say that phishing is any attempt on behalf of a cybercriminal to steal credentials. This can be carried out via a phishing website where the victim is prompted to enter his credentials or via a malicious executable.

Leading organizations in Phishing research, such as APWG (www.APWG.org) categorize a malicious threat as phishing according to the following two rules:

1. If the page is representing a brand and asks for any login/personal information.

2. If the URL is not say "companyname.com, and if you do a whois on it, the domain is not registered to that company name. So if the URL is ilikepuppies.com and displays the logo of a major brand, it is trying to make itself look like that major brand.

What's the difference between Phishing and Malware?

The relationship between phishing and malware is a bit blurry, mostly because they often work together to achieve the goal of the cybercriminal. In fact, the term "malware" is often included in phishing discussions.

Now that being said, here is Wikipedia's malware definition:

"Malware, short for malicious software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software."

"….Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses…."

One key distinction is that not all malware is delivered via email. Malware converges with phishing when it is being used as an accessory to execute the phishing attempt.

In addition to thorough adversary analysis, what else can be done to get in the way of phishing criminals and break the phish chain?

You've probably heard the popular Chinese Proverb that states "Give a man a fish and you feed him for a day. Teach a man to fish and you feed him for a lifetime." This idea holds true when it comes to helping and teaching your customers what they can do to protect themselves from becoming the victims of a phishing attack. While you can spend your time focused on taking down phishing sites, one by one, your customers will continue to click on the next site that comes along. While it may not be a site targeted at your brand and may not affect you directly, your customer will suffer. The more that brands create public awareness about how consumers can avoid becoming victims of phishing attacks, the better.

There are a few tactics that help customers avoid phishing victimization:

- Security education
- Anti-malware toolbars
- Secure web app training (for pwned site admin)

How Phishing Costs Your Organization

Of course, one man's loss is another man's gain. If you are in an enterprise environment, there are significant costs that you are likely to incur as a result of a successful phishing attack. You've got to really understand and think about what this is going to mean to your specific environment. Phishing costs you in a number of ways:

- **Financial loss:** When a cybercriminal steals from you, you've got to make good on it because you can't alienate and antagonize the customer (even if they played a role in the attack). In the age of the Internet and social media, it is easy for the incident to become publicized if it is not handled properly.
- **Clean-up costs:** You've got to clean up the mess, so if there's some kind of attack where someone has compromised your back-end systems or someone has compromised the consumer in some way, you may have to step in to help them fix it.
- **Brand damage:** In any cyber attack, you will ultimately deal with brand damage as well. Unfortunately, when brand reputation is damaged it yields long-term consequences, as consumers lose confidence and trust in your brand and often choose to take their business elsewhere.

Size of Organization	Monetary Loss*	Remediation Cost*	Reputation Cost*
Up to 1,000 users	$327	$558	$2,346
Between 1,000 and 5,000 users	$233	$484	$1,436
More than 5,000 users	$290	$833	$1,553

*Per Infected User

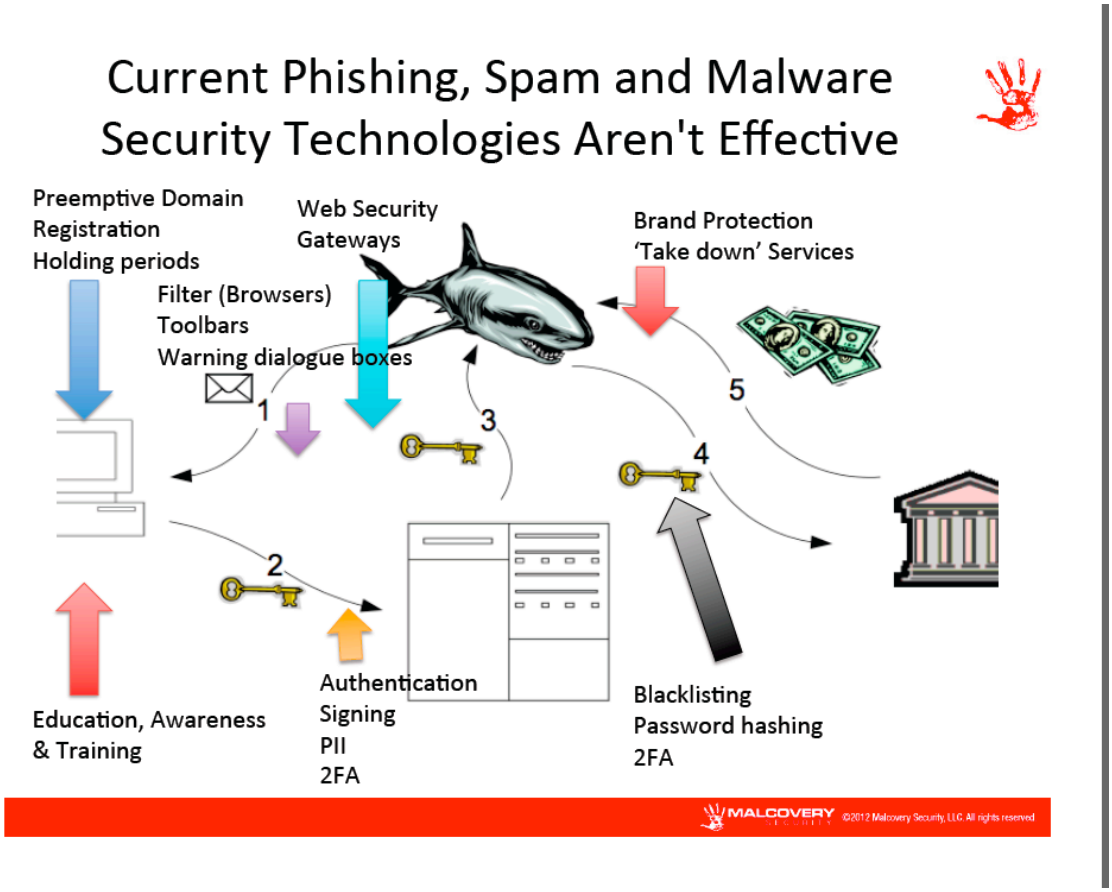
How Can I Protect My Company and My Brand Against Phishing?

Phishing is not a new problem. Almost 20 years from its 1996 beginning as a nuisance to America Online subscribers, the practice of impersonating a trusted brand via email to trick naive or unsuspecting users into visiting malicious websites is still going strong. What's more, this approach, one that essentially automates social engineering, brings with it unprecedented economies of scale.

There are many different technologies that also are in the 'food chain' for providing protection against phishing, including:

- Security Awareness Training (Education & Training)
- Filters (spam, phishing)
- Web filtering
- Forensic services
- Takedown services
- Standards/DMARC

If we look at these technologies as anti-phishing solutions, they all have one thing in common: they deal with the symptoms of phishing, and they do not dress the root source /root cause issues. As a result, each provides some deterrent or protection to phishing issues, not none address the cause--the source and nature of the cyber attack-- and therefore cannot address holistically the countermeasures to prevent, detect and respond to exiting and future phishing attacks.



This is not to disparage any of these solutions. Each can be a viable *part* of the solution to combatting phishing. However, by looking at 'root cause analysis' for phishing, battling phishing can be fundamentally more successfully.

Root cause analysis practice allows solving problems by identifying the root causes of events, as opposed to simply addressing their symptoms. By focusing correction on root causes, problem recurrence can be prevented. Root cause failure analysis recognizes that complete prevention of recurrence by one corrective action is not always possible. Conversely, there may be several effective measures (methods or countermeasures) that address the root causes of a problem. Thus, root cause analysis is often considered to be an iterative process, and is frequently viewed as a tool of continuous improvement.

How to Break 'The Phish Chain'

You can continue to disrupt phishing through the methods discussed that address simply the symptoms of phishing, such as traditional takedown methods. But, it's a short-term fix. A long-term to fix to the phishing problem requires serious commitment on behalf of your brand.

In order to break the phish chain, you need to commit to:

- Track phishing sites
- Identify attackers
- Prioritize attacks (based on risk)

A long-term fix to phishing requires you to treat the root cause, which will protect your customers and your brand through an in-depth understanding of your adversaries. While you can engage in phishing take down, several new phishing sites will launch for every few that you take down. Every day will be like the movie 'Groundhog Day.'

Remember, every minute that a phishing site is live will cost your customers money, which may eventually cost you money. Can you afford not to break the phish chain?

Ready to Break the Phish Chain?

In order to break the phish chain, we need to gain an understanding of how the cybercriminal is attacking us. For this, we use threat intelligence dissect and profile phishing kits. Ultimately, we want to identify the attackers and track the malware being used.

When we are able to identify patterns, isolate specific attacks and recognize malware, we gain the ability to help our customers protect themselves. Even in the case where our customers fall victim to an attack, phishing intelligence allows us to respond quickly and effectively to minimize the damage, take down phishing sites and stop the criminal from future attacks.

Phishing intelligence (and the process, which we will deinfe in depth in the next section) is produced through an examination of large amounts of email to identify trends and emerging patterns, aka big data analytics. While the term "big data" has quickly earned its place

among other buzz words, it provides for a scalable mechanism to understand the who, what, where and why behind phishing attacks, profile phishing kits, identify attacks and track malware.

The key questions answered by phishing intelligence: The 5 W's

Who? Who is attacking you? The majority of phishing attacks can be attributed to a select few phishing organizations that are highly skilled and efficient. If we can identify them, we can predict the tactics that they will use and the capabilities that they can use to target us in the future. This allows us to respond appropriately and defend ourselves effectively.

What? We need to understand the capabilities available to the attacker in order to develop a profile of the attacker over time by analyzing the malware that they are using. Are they using phishing kits? How have they changed? How have their targets changed? Are they going after specific banks or are they diversifying their efforts to target more consumer brands? This information gives us perspective about what they may be targeting next – and it may be you.

Where? Where does the attack originate? When a message is delivered, it contains links that lead to s*omewhere*. Where does it go? When a device is compromised and is communicating with the command and control infrastructure, how are they doing it? Are you tracking domains? What kind of IP connection patterns are there? Hackers today are using very sophisticated methods to connect compromised devices to their malware and botnet. The goal is to gather a dossier on the attacker so that you can go to law enforcement or use other channels to stop the attacker.

When? Why are we interested in when these attacks happen? It gives us a perspective of how we're going to protect ourselves and understand when we need to have our defenses in place. Answering this question requires human intelligence in order to provide historical context.

Why? The most important thing to identify as a result of the adversary analysis (who?) is the motive. Is it a targeted attack? If you are an enterprise being targeted for your intellectual property, that's an entirely different scenario than someone trying to steal customer account credentials.

The Phishing Intelligence Process Defined

As we discussed earlier in this paper, all other antiphishing technologies and methods deal with symptoms and by their very nature are reactive. Using actionable intelligence to prevent fraud loss is proactive. Today's cybercriminals are launching targeted attacks against your brand with speed and efficiency. In order to meet them, you'll need to operate with more speed and efficiency than you have before. It's time to challenge the status quo and adopt a proactive approach to fighting phishing attacks against your brand. There is a need for a holistic approach to phishing that seeks out and verifies phishing sites using many available sources, collects all forensic information, and uses computer science techniques to correlate all of the data.

The Phishing Intelligence Process

Step 1: Identify sites as "suspicious"

The first element of this process is intended to help you discover hundreds more phishing sites each day than are otherwise known. For example, your organization may collect information from a handful of sources regarding suspected phishing web sites. Again, this is a reactive approach. Phishing intelligence actually goes hunting for such sites by collecting not only from the traditional sources but also thoroughly collecting the original spam messages that disseminate the links to the sites. Links are then extracted and analyzed in real time. Your phishing intelligence tools should also address the servers of other phishing sites, checking several places on compromised servers to reveal other phishing sites.

Step 2: Verify suspected sites as "fraudulent"

This is where we determine which online service provider brand is being spoofed. A fast and accurate labeling process allows the takedown process to begin much earlier. Your phishing intelligence service identifies phishing sites targeting your brand, notifying your takedown vendor immediately. This keeps you ahead of the clock and saves your internal team the time and personnel costs of visually verifying phishing sites. And with early and accurate warning, your anti-fraud staff can also respond more efficiently, injecting incident intelligence back into your own systems and allowing a comprehensive understanding of the level of fraud losses for a particular criminal. Our experience has shown that the quick and accurate identification of related losses is necessary when referring a case to law enforcement.

Step 3: Collect digital evidence

Meanwhile, all of the digital evidence is collected in a forensically sound manner. In the phishing intelligence process, all of the files used to create a phishing web site that are being hosted on a fraudulent location (either the phisher's own host or a compromised host) are downloaded to phishing intelligence servers and archived. A unique identification number is assigned to each phishing incident, and all of the components of the incident are recorded, including the unique MD5 hash value for each component file. Using these unique values, your phishing intelligence service can confirm the identity of each component file and also analyze it for distinctiveness. Many phishers re-use several files found elsewhere on the Internet, changing only a portion of the file as needed. A patented algorithm takes these files apart and determines which portions have been

altered so that the files can be compared more accurately to files from other, known phishing sites. This type of analysis allows for the systematic assignment of a targeted brand to a phishing web site and provides to you and your company the most thorough volume of phishing intelligence available.

Step 4: Correlate the data

The final real-time element in the phishing intelligence process is to correlate the data among all known phishing sites toward helping you prioritize your investigative dollars. Using sophisticated innovations in clustering techniques that have their genesis in the identification of hidden infections in hospitals, you can gain immediate access to how each phishing site is linked to other phishing sites.

Step 5: Learn to recognize future sites

The end of the process is the time to analyze your results and identify trends and lessons learned as they apply to targeted attacks against your brand. Use this information as you begin the process again to fight future attacks.

Want to Learn More?

Want to Learn More?

Phishing remains a growing problem and a persistent threat. The total number of phishing attacks in 2012 was 59% higher than 2011 and global losses to phishing were estimated to be $1.5B in 2012. Many of today's current solutions, such as education and training of end users, web filtering, two-factor authentication, phishing takedown services, are proving to be only partially effective.

How can we be more effective, then, at fighting this problem, which costs our organizations in both time, money and brand reputation? Phishing Intelligence is the answer.

Intelligence will allow you to:

- Differentiate between the criminal who is a repeat offender, as opposed to an "ankle biter" amateur.
- Prioritize which criminals to investigate based on those who pose the greatest threat.
- Pinpoint the sources and nature of criminal activities in order to prevent future attacks.
- Determine if a phisher campaign is increasing, decreasing, or shifting to new attack tools.
- Identify emerging threats in order to protect yourself ***before*** you are infected.

In other words, you don't have to play "whack-a-mole" anymore.

Malcovery Security is the leading provider of actionable cyber security intelligence and forensic analysis, delivered through software and services that target cyber criminals and their activities. The company's patented and patent-pending technology provides the ability to identify the root sources of cybercrime attacks (servers, perpetrators, locations, etc.), delivering rich actionable intelligence information about cross-brand attacks and targeted attacks, as well as advanced notification of emerging e-mail-based threats.

Unlike services that serve only as a reactive response to these attacks today--services that simply address the symptoms, but cannot provide the intelligence to actually stop the cybercriminal--Malcovery Security's solutions provide the unique intelligence required to respond effectively to attacks on customers' brands, to disrupt phishing activities and successfully prosecute cybercriminals.

Malcovery Security is based on technologies developed at the UAB Center for Information Assurance and Joint Forensics Research (CIA|JFR) and has offices in Pittsburgh, PA and Birmingham, AL.

For more information, please visit http://www.Malcovery.com or connect with Malcovery on Facebook (facebook.com/malcovery), Twitter (twitter.com/malcovery) and LinkedIn (http://www.linkedin.com/company/malcovery-security)