

# BEST PRACTICES FOR PROTECTING AGAINST PHISHING

## MANAGING AN EFFECTIVE COMMAND CENTER IN THE FIGHT AGAINST ONLINE FRAUD

White Paper



TERMS SUCH AS PHARMING, TROJANS AND MAN-IN-THE-MIDDLE ATTACKS ARE GENERATING MORE AND MORE “BUZZ” IN THE FINANCIAL INDUSTRY. WHILE IT IS PARAMOUNT FOR FINANCIAL INSTITUTIONS TO STAY AHEAD OF THESE EVOLVING THREATS AND THEIR POTENTIAL IMPACT, PHISHING REMAINS THE PREDOMINANT TECHNIQUE FOR EXTORTING CONSUMERS OF THEIR PERSONAL INFORMATION AND FINANCIAL DATA ONLINE. THE VERY REASON PHISHING REMAINS SO PERVASIVE IS BECAUSE IT IS STILL VERY EFFECTIVE; AS FINANCIAL INSTITUTIONS ENHANCE THEIR LEVEL OF ONLINE PROTECTION, AND AS CONSUMERS BECOME MORE AWARE OF PHISHING, NEW AND MORE SOPHISTICATED ONLINE FRAUD TECHNIQUES WILL BEGIN TO TAKE HOLD.



The Security Division of EMC

Today, with thousands of phishing attacks every month, targeting hundreds of global financial brands, it is important for financial institutions to protect themselves and their customers first and foremost against phishing, while preparing in advance and putting additional measures in place to combat more sophisticated attacks as well. The single most effective way for an organization to reduce the impact of phishing and protect its brand, customers and assets is to shut down fraudulent websites. Although additional protection mechanisms certainly exist and should be leveraged, disabling a phishing site simply stops the attack. This ensures that the fewest consumers—who are duped by a phishing email into clicking on a link to a fraudulent site—are actually defrauded after landing on the spoofed site.

This then begs the question: What is the best way to effectively shut down fraudulent websites? This paper establishes several best practices that financial institutions—or any organization faced with phishing—can take to >



effectively disable fraudulent websites and explores the importance of managing an effective command center when combating phishing.

### **The Importance of Managing an Effective Command Center**

There are various ways to combat phishing. The most suitable approach combines several measures, technologies and services that take place in parallel in order to mitigate a phishing attack as quickly as possible. Whether a financial institution selects to deploy anti-phishing measures using its own resources, or selects an outsourced service, dealing with phishing is a process that requires expertise in the areas of phishing specifically and online financial fraud in general.

The most common approach in the industry for dealing with phishing attacks includes the establishment of or partnering with a command center that is geared towards handling the attacks from the point of detection until the eventual shutdown of the attack. One might assume that establishing a command center is quite simple and mainly a matter of logistics and resources, however the name of the game in combating phishing is speed and efficiency – the difference between an inexperienced command center and a well-oiled machine can easily be seen in the number of victims and amount of damage caused by a given attack.

Therefore, when establishing a command center, or looking to outsource phishing site shutdown to an existing command center, it is critical to take the command center's experience and track-record into consideration. One can verify the efficiency of a command center by simply putting it to the test: How fast does the command center detect the attack? How long does it take to shut down a live phishing attack? How much compromised information and intelligence does the command center uncover when analyzing an attack? And so on.

Additional things to take into consideration include the number of attacks that the center has effectively taken down, the effectiveness of the phishing attack handling process and the amount of institutions supported by the

center. Just as important is the center's specific anti-fraud expertise. Since phishing is only one instance of online financial fraud, experience and know-how in financial services and anti-fraud measures is extremely important when dealing with phishing. An effective command center should consist of experienced fraud analysts that undergo extensive training and ongoing education regarding new fraudster techniques and financial fraud methods.

Once the command center is up and running, there are several best practices that can be taken to ensure its ongoing effectiveness.

### **The Flow of a Typical Attack**

Handling phishing attacks is a resource-intensive, time-consuming process that includes various skills and tools in order to be successful (see Figure 1). As described above, the first recommendation when dealing with phishing attacks is to establish or leverage an existing command center.

Before we dive into the best practices, we will describe the general flow of handling a phishing attack. The first step that needs to take place is detection – you can't work to shut down an attack unless you know that it is taking place. The faster you discover an attack, the faster you can work on disabling it. The most effective way to detect phishing attacks is to leverage multiple sources. For example, one can partner with anti-spam providers who scan mass amounts of emails per day as well as allow consumers to report that they have received a phishing email.

Once an attack is identified, one should commence working to shut down the fraudulent website. This is typically done by contacting the hosting facility where the site is being held. The shutdown process includes several tools and steps including locating the relevant hosting facility, finding the right contact information and the right person to speak with, explaining the matter in the right language in a clear manner and sending a Cease & Desist legal form demanding to shut the site down. It sounds simple enough, but trust relationships within the hosting organizations are critical to the speed and

success of site shutdown and are only established over time. Once the site is offline, ongoing monitoring should take place to ensure that it is not revived and re-launched.

### **Best Practices for Disabling Phishing Sites**

Below we have included several additional best practices that help to ensure an effective command center and rapid detection and shut down of fraudulent websites. These recommendations are a result of the experience gained by RSA's Anti-Fraud Command Center (AFCC). The AFCC is a 24x7 war-room that detects, monitors, tracks and shuts down phishing, pharming and Trojan attacks against over 100 institutions worldwide. The AFCC, which is staffed by more than 40 trained fraud analysts, has shut down over 18,000 phishing attacks and is a key industry source for information on phishing and emerging online threats.

#### **1. Establish a Global Operation**

Every hour that a phishing site is live, a financial institution runs the risk of its customers divulging their information and falling victim to fraud. Time is of the essence. An anti-phishing command center must prepare as much as possible in advance for an attack and the shutdown process. It also must ensure that it has the resources and expertise to handle phishing globally. For example, because phishing is conducted on a global scale and attacks are hosted in more than 70 countries worldwide, the command center should have multi-lingual capabilities. This can be achieved by hiring fraud analysts that are bi-lingual (at least) and pre-translating documents that are used in a shut down scenario. If the command center handles phishing attacks, pharming attacks and brand abuse attacks, and it submits Cease & Desist letters as part of the shut down process, then it should have the letters for each type of attack already prepared and translated in the relevant languages so that all the fraud analyst has to do in real-time is send the appropriate letter.

Another tool to prepare in advance and achieve global coverage is an immediate-response translation company that can assist

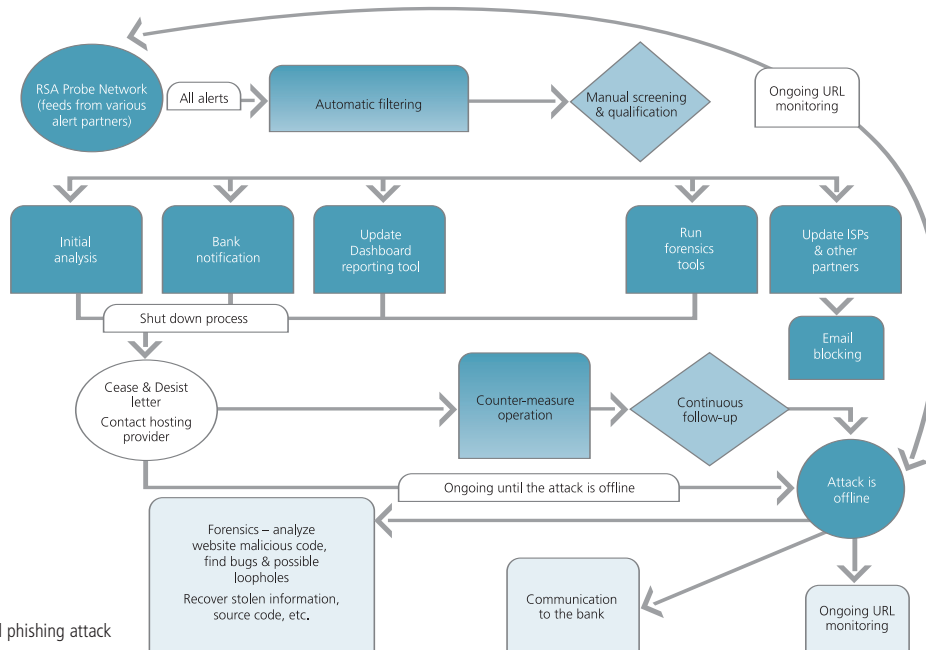


Figure 1  
The flow of a typical phishing attack

in translating on live phone calls with hosting facilities around the world. It may not be realistic to find fraud analysts that cover 70 languages, but it is practical to train the analysts to contact a real-time translator and conduct a conference call with a facility anywhere in the world.

A command center should have all standard communication messages prepared in advance, such as phone scripts and email templates – a fraud analyst should not have to type out the definition of phishing from scratch every time she encounters a new hosting facility. In short, the more preparation done in advance, and the more tools and resources put in place in order to have global coverage, the easier the shut down process will be for the fraud analysts and the faster the site can be shut down.

## 2. Use 24x7 Threat Response

When shutting down phishing attacks, it is critical to be on alert at all times. A phishing shutdown service must be a 24x7 operation. Fraudsters conduct phishing in order to make money. They look for any vulnerability they can find, including attacking people when they least expect it. For example, one might see a surge in phishing attacks after business hours, or on weekends, when financial institutions and

hosting facilities are either closed or understaffed. This could slow down the shutdown process and extend the fraudster’s “window of opportunity”. Additionally, there is often an increase in attacks hosted in a certain country that has a national holiday and therefore businesses are slow-moving.

A command center that works round the clock ensures that regardless of the attack’s time zone, the fraud analysts are fully operational and working to shut it down.

## 3. Connect with Hosting Facilities, Build and Maintain Relationships

When phishing first surfaced on the Internet in 2003, shutting down a site could take several days, if not weeks. Due to the low awareness of the problem, hosting facilities were skeptical and hesitant when asked to shut down a fraudulent site. After all, an ISP hosting a site has a reputation to uphold, it can’t simply dismantle its customers’ sites on a whim, at least not if it wants to stay in business. Today, awareness has increased, which helps in communicating with hosting facilities. Thus, a command center that has established relationships with hosting facilities will have an advantage and will be more successful in fast site shutdowns.

There are various types of hosting facilities used to host phishing attacks – starting from ISPs, free and commercial web hosting companies, registrars and Internet email providers such as MSN Hotmail, Yahoo! and the like. When working to shut down phishing sites, it is important to be familiar with the various workings and intricacies of the Internet, in order to understand where the site is located and contact the right entity during the shutdown process.

Shutting down fraudulent sites is not an exact science, and therefore it is critical to learn from experience and log information that is learned. For example, fraudsters tend to use the same hosting facilities over and over as long as it suits their needs, so once the fraud analysts at the command center have found the right person to speak with at the hosting facility and have successfully shut down a site hosted at the facility, they should save all of the contact information and any additional tips for working with that specific hosting facility for future use. A large database of hosting facility contact information and helpful tips can significantly shorten the time it takes to shut down a site in a subsequent attack. As the command center becomes more experienced in site shut downs, it can reach a very high success rate of shutting



down a site within minutes to very few hours when dealing with a familiar hosting facility. Ideal situations include having the cell phone and email address of the most relevant person at a certain hosting facility and simply sending a quick request with the fraudulent URL, and the site is disabled immediately.

Maintaining the relationships that are built with the different hosting facilities is also important. No doubt that a hosting facility will be more cooperative and helpful, increasing the shutdown success rate, if the team there is familiar with the command center and appreciates its professionalism and expertise.

It also makes sense to establish connections and build relationships with the various law enforcement agencies and Computer Security Incident Response Teams (CSIRT) that deal with cyber security and online fraud. This is a best practice for combating online fraud in general, but can also be useful specifically when shutting down sites. In some countries the hosting facilities tend to be much more cooperative in disabling fraudulent sites when the request is made by a law enforcement or federal agency. Therefore, a command center with those relationships will have an easier time and be more successful in shutting down sites located in certain countries.

#### **4. Stay In Tune with New Attacks and Fraud Techniques – Build Ongoing Expertise**

From the very beginning of establishing a command center and shutting down phishing sites, it is important to find and leverage talented and experienced fraud analysts. While it might seem like a simple task that just

requires persistence and good communication skills, operating a command center requires initial expertise as well as ongoing training, education and intelligence gathering.

Important background information and characteristics for fraud analysts include: education in the areas of computer science and engineering, wide experience in the technical environment of the Internet (networking, infrastructure, TCP/IP protocol, software and hardware routing), and experience in providing technical support. It is also helpful for each fraud analyst to be bi-lingual. Once the right analysts are found, extensive training and ongoing education will ensure that the command center remains efficient.

Phishing and online fraud are constantly evolving. Fraudsters become more sophisticated every day and conduct a great amount of information sharing via online fraudster forums and communities. It is imperative for a command center to stay in tune with developing fraud and phishing trends in order to detect and shorten the lifespan of attacks as they change. Ongoing educational workshops, bi-weekly meetings where the team shares information and “war stories,” monitoring of fraudster communities and updated analysis of phishing attacks and their infrastructure can help ensure that the fraud analysts are constantly up-to-date and effective in their work.

#### **5. Work in Parallel**

There are a multitude of pieces to the puzzle when fighting phishing – from detection of attacks, to analysis, site shutdown, blocking via ISPs and anti-spam partners, forensic work digging for data and

compromised information, and more. The most effective anti-phishing service deploys as many technologies and methods at once as possible. Even with all best practices in place, sometimes it can take many hours and even days to shut down a phishing site. In the meantime, there are other things that can and should be done in parallel to mitigate the damages of an attack.

One good example of an anti-phishing counter-measure that can be operated simultaneously with the shutdown process is site blocking. By partnering with ISPs and anti-spam providers, a command center can feed fraudulent URLs to the blocking partners, which then block access to the phishing site for their customers. In other words if a command center feeds a phishing site to a major ISP, then all members using that ISPs Internet browser will not be able to reach the phishing site. Even if they proactively clicked on the link in the phishing email, they will receive a message that the site is blocked since it led to a phishing site that contains malicious content. This blocking process provides protection to consumers while the command center works to shut the site down completely.

#### **About RSA Inc.**

RSA Inc. is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the Company leads the way in strong authentication, encryption and anti-fraud protection, bringing trust to millions of user identities and the transactions that they perform. RSA's portfolio of award-winning identity & access management solutions helps businesses to establish who's who online – and what they can do.

With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve more than 21,000 customers – including financial institutions representing hundreds of millions of consumers around the globe – and interoperate with over 1,000 technology and integration partners. For more information, please visit [www.rsasecurity.com](http://www.rsasecurity.com).



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

**The Security Division of EMC**

**RSA CONSUMER SOLUTIONS**

©2006 RSA Security Inc. All rights reserved. RSA, and RSA Security are trademarks or registered trademarks of RSA Security in the U.S. and/or other countries. All other products and/or services are trademarks of their respective companies.