RSA®

The Security Division of EMC

White paper

Phishing, Vishing and Smishing: Old Threats Present New Risks

How much do you *really* know about phishing, vishing and smishing?

Phishing, vishing, and smishing are not new threats. They have all been around for years, but it is the way that online criminals use these tools to scam unsuspecting consumers that have changed.

Some researchers have argued that the use of these tactics is diminishing and being replaced by far more advanced attacks such as Trojans. However, RSA has witnessed an increase in these attack vectors in recent months. For example, in August, September, and October of 2009, RSA reported record-breaking numbers of phishing attacks detected by the Anti-Fraud Command Center[1].

Phishing, vishing and smishing remain popular within fraudster circles for a number of reasons. First, the execution cost to launch an attack is very low which greatly reduces the barriers to entry for a new fraudster starting out. Second, little technical knowledge is required to set up an attack. The setup process has become entirely automated and a phishing attack can be launched in a few clicks. Finally, they still work. While the tactics that fraudsters use are different, consumers are still tricked into divulging their personal information online and over the phone.

This white paper will examine the latest methods fraudsters are using to launch phishing, vishing, and smishing attacks, why they continue to be successful and what consumers can do to protect themselves.

Contents

[1] *RSA Monthly Online Fraud Report*, September, October and November 2009

I. Phishing

One of the earliest known phishing attacks can be traced back to 1996 with hackers trying to steal America Online passwords from online users. A phisher would pose as an America Online staff member and send an instant message to a potential victim requesting his password. In order to lure the victim into giving up sensitive information, the message might include a call to action such as "verify your account." Once a password was revealed, phishers would use the victim's account for fraudulent purposes or to spam other online users.

Consumer awareness concerning the threat of phishing has increased over the last few years, reducing the response rate to standard phishing emails and in turn, the overall effectiveness of an attack. For example, in 2006, the Anti-Phishing Working Group reported that the average lifespan of a phishing attack was 108 hours. In 2009, that same average has decreased by over 50% to 52 hours[2].

This has forced fraudsters to develop new innovative ways to launch phishing attacks – from the backend systems and tactics they use to launch an attack to the online users they target.

Fast-flux networks

Fast-flux networks are one of the methods that fraudsters are using to extend the life of a phishing attack. First used by the notorious group RockPhish, fast-flux is an advanced Domain Name Server (DNS) technique that utilizes a network of compromised computers, known as a botnet, to hide the true origin of the content server (usually referred to as the "mother ship") that hosts phishing websites. The botnet acts as an army of proxies, or middlemen, between the user and the website.

Exposing and shutting down attacks hosted on a fast-flux network is theoretically more difficult as the content server that is hosting the attack hides behind a cloud of compromised computers, thus the IP address is constantly changing. Since April 2009, 57% of all phishing attacks identified and shut down by RSA were hosted on fast-flux networks.

Drive-by-downloads

Historically, phishing and Trojans have been recognized as two unique means of attack. However, the use of a standard phishing attack to infect users with a Trojan is becoming more prevalent among fraudsters – a natural evolution that is driving propagation of Trojans to a much higher degree. This is accomplished through what is known as a "drive-by download,"[3] and social engineering plays a key role in the success of these attacks.

A typical ruse used by fraudsters is to take a current topic or a popular celebrity that is in the news or of high interest to the general population. Fraudsters send emails to unsuspecting users directing them to view a video or read a news article. When users click on the link or the video, they are infected with a Trojan.

In April 2009, the official website of musician Paul McCartney was hacked for two days (see Figure 1). When visitors accessed the site, their machines were hit with an exploit that downloaded a Trojan rootkit. Once the rootkit was installed on the computer (unknown to the victims), fraudsters were capable of logging a user's keystrokes at every website they visited and collecting personal information such as credit card details and login credentials.

> Phishing, vishing, and smishing have all been around for years, but the way that online criminals use these tools to scam unsuspecting consumers has changed.

[2] *Anti-Phishing Working Group*, "Phishing Activity Trends Report, 1H 2009"
[3] A program that is automatically downloaded to a user's consent without their consent or knowledge. The download can occur by simply visiting a website or viewing an email.

Figure 1: Visitors to the Paul McCartney website were warned they may have been infected with a piece of malware.

Spear phishing and whaling

Spear phishing, or whaling, is a form of phishing attack that is mainly targeted at employees or high-profile targets in a business. Spear phishing emails attempt to get a user to divulge personal or sensitive information or click on a link or attachment that contains malicious software. Once the user clicks on the link or attachment, malware is installed, usually in the form of a key logger, which is capable of stealing anything the user types including corporate credentials, bank account information or other sensitive passwords.

They are often harder to detect because they use information to make an employee believe that the e-mail is coming from their employer (such as the IT department), a colleague or another genuine entity. RSA uncovered a post in the underground that shows a fraudster soliciting the email addresses of a company's CEO and top executives and is willing to pay $50 for them (see Figure 2).

Incidents of spear phishing are increasing so rapidly, especially among small and medium-sized businesses, that the U.S. Federal Bureau of Investigation (FBI) recently issued a statement warning the public of the threat. It is estimated that as of October 2009, this type of fraud has created close to $100 million in attempted losses[4].

Figure 2: A post by a fraudster seeking the email address of top company executives.

[4] *Internet Crime Complaint Center*, "Compromise of User's Online Banking Credentials Targets Commercial Bank Accounts," November 3, 2009

Spear phishing attacks are highly clever and well researched. They are capable of fooling not just the users they target, but the enterprise controls that are designed to stop them. For example, in October 2009, researchers conducted a study[5] that sent a spoofed LinkedIn invitation email that appeared to come "on behalf of Bill Gates" to users in different organizations. The fake message evaded major email security products and controls at the organizations tested 100 percent of the time.

Chat-in-the-Middle

In September 2009, RSA discovered a new phishing tactic being used by fraudsters. Coined Chat-in-the-Middle because of the addition of a bogus live chat support window, this type of phishing attack attempts to obtain additional information from the user via a live chat session initiated by fraudsters.

The phishing attack starts out as a normal phishing website that prompts customers for their usernames and passwords. In a standard phishing attack, a user is redirected either to the next page (or pages) of the phishing website or to the genuine bank website after they provide a username and password. However, a Chat-in-the-Middle phishing attack proceeds with a fake live-chat support window. During the live chat session, the fraudster behind the attack presents himself as a representative of the bank's fraud department and attempts to trick customers who are online into divulging sensitive information - such as answers to secret questions.

II. Vishing

Phone phishing, or vishing, is the criminal practice of using the telephone system to gain access to personal and financial information from customers for the purpose of committing fraud. Vishing exploits an individual's trust in telephone services, as the victim is often unaware that fraudsters can use methods such as caller ID spoofing and complex automated systems to commit this type of scam. Yet as the yield on traditional phishing attacks continues to diminish, fraudsters have turned to vishing in an attempt to steal user's financial account numbers, passwords and other personal data.

The FBI issued a warning that exposed one of the many techniques being used by fraudsters to commit a vishing attack. Taking advantage of a vulnerability in public branch exchange (PBX) systems, fraudsters can connect to Voice over Internet Protocol (VoIP) services and "auto-dial" thousands of people in just an hour.

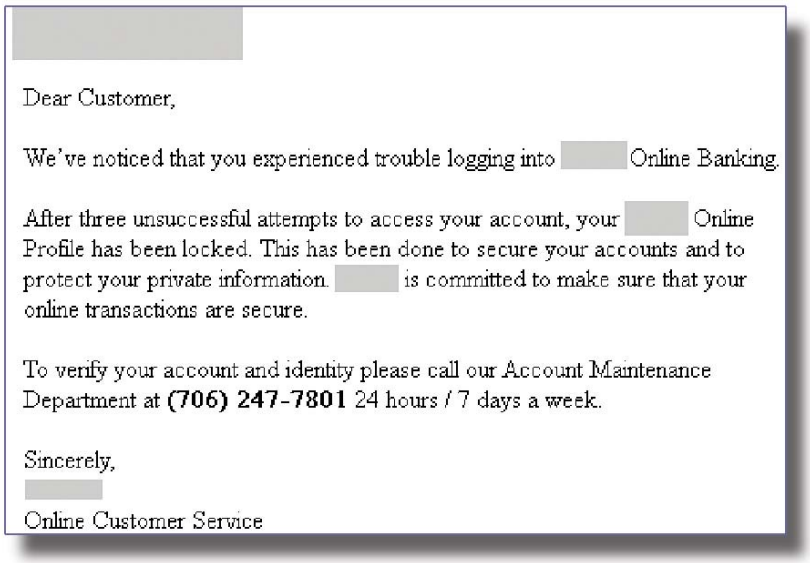
The typical process used when committing a vishing attack through an automated phone call is as follows:

1. A "war dialer" is used to call phone numbers in a given region or a legitimate voice messaging company with a list of phone numbers stolen from a financial institution.
2. When the consumer answers the call, an automated recording alerts the consumer that fraudulent or suspicious activity has been detected on their credit card or bank account. The message instructs the consumer to place a call to the bank immediately and provides a false phone number. Often time, this is also the phone number that is displayed on the caller ID screen.
3. When the victim calls the number, automated instructions request that they enter their credit card or bank account number into the key pad. However, the call can also be used to harvest additional details such as personal identification numbers, expiration date, CVV number and date of birth.
4. Once the consumer enters the requested data, the fraudster has the information necessary to make fraudulent use of the card or to access the account.

Some sophisticated attacks combine vishing and traditional phishing in which a phishing email is sent to an online user stating there has been a problem with an online account and appears to be from a legitimate company such as a bank, credit card company, or online retailer. The email then directs the user to call a number and enter certain information to verify their account (see Figure 3).

As is the case with spear phishing, small and medium-sized businesses have been particularly affected by the threat of vishing. Since the beginning of 2009, nearly 60% of the vishing attacks that RSA has addressed have been targeted at credit unions and small regional banks.

[5] "Major Secure Email Products And Services Miss Spear-Phishing Attack," *Dark Reading*, October 2009



Dear Customer,

We've noticed that you experienced trouble logging into [redacted] Online Banking.

After three unsuccessful attempts to access your account, your [redacted] Online Profile has been locked. This has been done to secure your accounts and to protect your private information. [redacted] is committed to make sure that your online transactions are secure.

To verify your account and identity please call our Account Maintenance Department at **(706) 247-7801** 24 hours / 7 days a week.

Sincerely,

[redacted]

Online Customer Service

Figure 3: An example of a vishing attack. In this example, the victim received an email that directed them to call a phone number.

III. Smishing

Smishing, or SMS phishing, sends a text message to an individual's mobile phone in an attempt to get them to divulge personal information. As is the case with phishing or vishing, a smishing attack usually has a call to action for the intended victim that requires an "immediate response."

Smishing is a growing problem for all banking segments including credit unions, regional banks and large nationwide banks. In particular, large nationwide banks have been the hardest hit by smishing as fraudsters can distribute their SMS spam to a wider base of mobile users who are more than likely to have some form of financial account at one of these institutions. Also, smishing is becoming a fraud tool of choice on a global scale as more consumers access the Internet through a mobile device or cell phone versus a traditional desktop or laptop PC.

The two most common types of smishing attacks are:

1. A person receives a text message that directs them to call a phone number to confirm personal or account information.
2. A person receives a text message that directs them to visit a website to confirm information, but is actually being served up with a malicious Trojan on their computer or mobile phone capable of stealing their passwords.

Smishing has become easier to do and a more attractive alternative to phishing. Success rates are higher with a smishing attack compared to a standard phishing attack as consumers are not conditioned to receiving spam on their mobile phone so are more likely to believe the communication is legitimate. Furthermore, whereas the majority of phishing emails are now stopped by spam filters and often never reach their intended targets, there is no mainstream mechanism for weeding out "spam" text messages.

As with vishing, fraudsters are also able to take advantage of legitimate services to target users of mobile phones. For example, there are services available that enable masses of text messages to be sent instantly from any computer to thousands of mobile phones. Fraudsters are also offering these services directly to other fraudsters, where they can pay a fixed price per thousand and send a custom text message to mobile users (see Figure 4). Fraudsters can also purchase software that spoofs the sender ID so that the text message appears to come from an email address originating at a legitimate entity.

Finally, smishing eliminates one of the many revealing factors that alert customers to a potential scam - misspelled words. In a phishing attack, it is easier for an individual to identify words that are misspelled in an e-mail, something that is rare in a communication from a legitimate entity. However, in today's mobile society, text messages are expected to be short because of character limitations so a misspelled word could be interpreted as an abbreviation, for example.

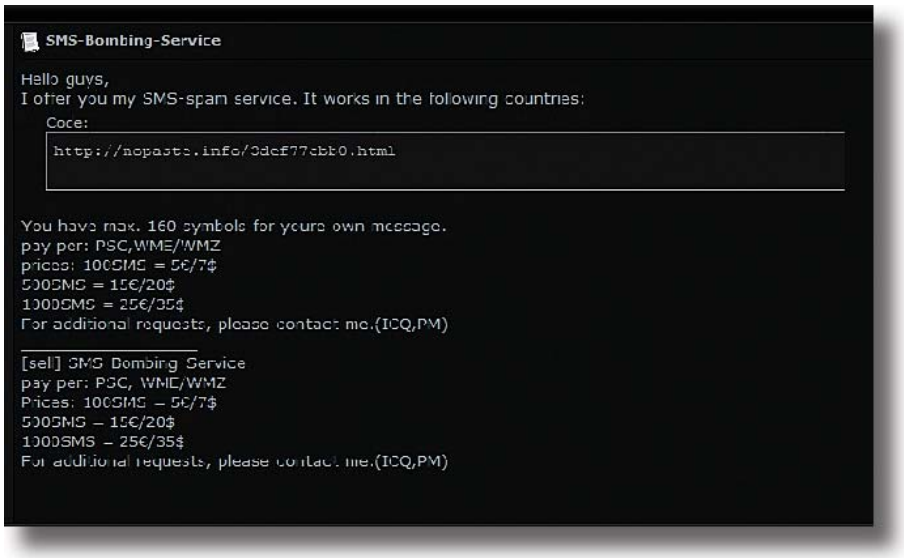


Figure 4: A fraudster is offering an SMS delivery service at a price of $35 per 1000 text messages

IV. Building Awareness

Building awareness of potential threats among consumers is critical to any mitigation strategy. There are many reasons for why fraudsters have evolved their tactics, but one of the key factors is increased awareness among their intended victims. Consider the evolution of phishing attacks and how advanced the methods used by fraudsters have become. This can be directly attributed, at least in part, to the vast awareness that exists among online users today.

In a recent independent study conducted by Infosurv and commissioned by RSA, over 4,000 online users in over 20 countries were surveyed about their awareness to a variety of online threats and their attitudes towards online security. An overwhelming majority expressed awareness of phishing scams compared to vishing and smishing scams (see Figure 4).

But awareness and education should no longer just be limited to consumers. As fraud extends into the enterprise, the same rules that apply to consumers must be extended to corporate users, as well. Some common online (and offline) safety tips are provided below:

- Never open an attachment or click on a link that comes in an email from someone you do not know. More than likely, the attachment or website contains a Trojan or other form of malware that is downloaded on your computer to steal your information.
- Never provide personal or financial information through an email or over the phone. Banks and other companies do not request you confirm personal information via email, over the phone or through a text message. They do not need to request identifying information because they already have that on record.
- Always know who you are dealing with online especially when it comes to your personal information. Just because an email, a text message or the pre-recorded message on your phone says it is your bank or some other organization you commonly deal with, it doesn't mean it is legitimate.

An overwhelming majority of online users in over 20 countries expressed awareness of phishing scams compared to vishing and smishing scams.

Response	20%	40%	60%	80%	100%	Freq.	Count
Phishing emails						75.9%	3444
Phishing via SMS / text message (“SMiShing”)						32.5%	1476
Phishing over the phone (“Vishing”)						25.5%	1155
Trojans						80.5%	3651
Keyloggers						26.4%	1198
Malware						54.3%	2464
Spyware						73.9%	3353
Adware						51.8%	2349
Botnets						14.0%	636
Viruses						88.1%	3999
Worms						65.1%	2953
Other						1.3%	58
						Valid Responses	4538
						Total Responses	4538

Table

Which of the following types of online threats are you familiar with?

- Guard your privacy and limit the amount of personal information you share online. Between the information available in public records and the personal information we willingly share online, fraudsters can easily gather the information they need to pretend they are you. They can also use this information to answer the challenge questions many online service providers require to access your account and/or retrieve or change your password.
- Check your bank and credit card statements regularly. Fraudsters are very sophisticated and even the most savvy consumers can fall for their scams. In order to keep your information and accounts safe, you should check your bank and credit card statements for suspicious activity on a frequent basis.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

PSV WP 1109 H11933