Fraud Alert: New Phishing Tactics—and How They Impact Your Business

Contents

Fraud Alert: New Phishing Tactics—and How They Impact Your Business

Introduction

Phishing remains a major security threat to businesses and their customers around the world—and the threat keeps rising. Compared to the last six months of 2011, the first six months of 2012 saw a 19 percent increase in global phishing attacks, with businesses suffering an estimated $2.1 billion in phishing-related losses between January 2011 and June 2012.[1]

Two factors are driving this increase: (1) phishing attacks are relatively easy to execute, and (2) they generally work. You don't need to be a sophisticated hacker to go phishing on the Internet. All it takes is a little motivation, malice, and greed, thanks to off-the-shelf phishing kits provided by a thriving cybercrime ecosystem. Cybercriminals are even using a business model known as malware-as-a-service (MaaS), where authors of exploit kits offer extra services to customers in addition to the exploit kit itself.[2]

Approximately 156 million phishing emails are sent every day, with some 16 million successfully passing through filters. Roughly 50 percent of the remaining emails—about eight million—are opened, with 800,000 users lured into clicking on a malicious link. Again, that's not 800,000 per year. *It's 800,000 per day.*[3] To combat such a massive volume of malicious email, it's more important than ever to stay current on the latest methods employed by cybercriminals. Only then can you take proactive steps to protect your business from fraud.

In this fraud alert paper, we'll highlight the current trends in today's phishing schemes, with a particular focus on the latest threats emerging from China. Then we'll offer some ideas and best practices for applying technology to protect both yourself and your customers.

Phishing Knows No Limits

Phishing—the act of luring unsuspecting people to provide sensitive information such as usernames, passwords, and credit card data via seemingly trustworthy electronic communications—is an ongoing global threat of massive scale and nearly unlimited reach.

The Anti-Phishing Working Group (APWG) reported at least 93,462 unique phishing attacks globally in the first half of 2012 in 200 top-level domains. That represents a significant increase over the first half of 2011, when APWG reported 83,083 phishing scams—an increase attributed to the prevalence of attacks on shared virtual servers. Some 64,204 unique domain names were affected in 1H2012, targeting 486 institutions in all (see Figure 1).[4]

BASIC STATISTICS

	1H2012	2H2011	1H2011	2H2010	1H2010
Phishing domain names	64,204	50,298	79,753	42,624	28,646
Attacks	93,462	83,083	115,472	67,677	48,244

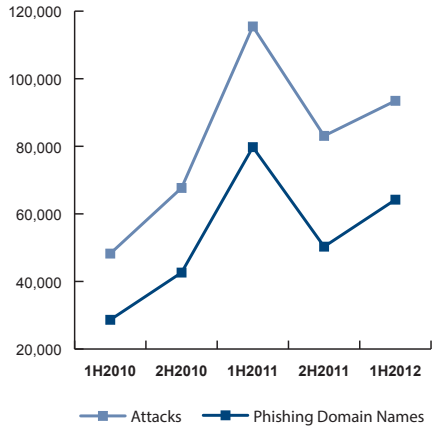

Figure 1. Phishing attacks keep trending up.

1. "Phishing and the Social World," RSA, October 2012.
2. "Verisign iDefense 2012 Cyber Threats and Trends White Paper," Verisign, January 2012.
3. "Phishing: How Many Take the Bait?," Get Cyber Safe, February 2013.
4. "Global Phishing Survey 1H2012: Trends and Domain Name Use," Anti-Phishing Working Group, October 2012.

Phishing in China: The Rise of APT1

The majority of phishing attacks appear to originate in China. This trend reached its peak in the first half of 2011, when Chinese phishers were thought to be responsible for 70 percent of all malicious domain name registrations worldwide.[5]

In February 2013, Mandiant published a report on a particularly destructive group of phishers allegedly operating out of China. Dubbed "APT1," this group—which has conducted Internet-enabled espionage against a wide range of victims since at least 2006—is almost certainly a government-sponsored campaign orchestrated by the Chinese People's Liberation Army (PLA). According to Mandiant's research, APT1 has stolen hundreds of terabytes of data from at least 141 organizations, and has the ability to steal from dozens of organizations simultaneously. These highly sophisticated phishers maintained access to each victim's networks for an average of 356 days, with one period of access to a single organization lasting for more than four consecutive years.[6]

Mandiant's findings reveal a great deal about the tactics, behaviors, and location of this particular group. In more than 97 percent of the instances in which APT1 intruders connected to their attack infrastructure, they used IP addresses registered in Shanghai, with all systems set to the Simplified Chinese language. In 767 separate instances, APT1 intruders relied on the HUC Packet Transmit Tool (HTRAN) to communicate between IP addresses and victims' systems, with all distinct IP addresses registered in China.[7]

The scale and sophistication of the APT1 threat appears to be without precedent. These phishers are clearly part of a large organization with possibly hundreds of human operators managing an attack infrastructure on more than 1,000 servers. Support staff would necessarily include linguists, malware authors, and top industry experts.[8]

A threat of this magnitude calls for robust, proactive measures to protect your business and your customers. To help bolster your defenses against APT1, Mandiant has released more than 3,000 indicators—including domain names, IP addresses, and MD5 hashes—available for download on Redline, the company's free host-based investigative tool. We encourage you to make immediate use of this valuable resource.

Shared Virtual Servers Remain a Prime Target

Last year, we reported a significant rise in phishing attacks on shared virtual servers. In these attacks, a phisher breaks into a web server that hosts large numbers of domains, then places the phishing content on every domain. As a result, every website on that server displays the phishing pages, thus infecting thousands of websites simultaneously.

These attacks diminished during the second half of 2011, but 2012 brought them back with a vengeance: in June alone, APWG reported a record 7,000 attacks on 44 different virtual servers.[9]

Spammers Continue to Take Advantage of Holidays and Global Events

In the run-up to Christmas 2012, spammers once again spoofed a number of legitimate retailers, offering Christmas "deals," gift cards, and other holiday bait. Some phishers took advantage of Americans' end-of-year tax anxiety by sending emails claiming to be from the IRS (Internal Revenue Service).[10] And as always, notable global happenings served as a trigger for a rash of scams—especially the 2012 Summer Olympics in London.

Anti-phishing experts expected to see a major increase in malicious emails leading up to the Olympics,[11] and scammers didn't disappoint. Over the course of the summer, Zscaler called attention to a rise in fake Olympic ticketing sites,[12] and Omniquad identified a "lottery scam" masquerading as a British Airways promotion for the London Games.[13] Expect to see similarly malicious attempts to exploit fans' enthusiasm for upcoming global sporting events like the 2013 FIFA Confederations Cup, the 2014 Winter Olympics in Sochi, Russia, and the 2014 FIFA World Cup in Brazil.

5. "Global Phishing Survey: Trends and Domain Name Use in 1H2011," APWG, November 2011.
6. "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 2013.
7. Ibid.
8. Ibid.
9. "Global Phishing Survey 1H2012: Trends and Domain Name Use," Anti-Phishing Working Group, October 2012.
10. "Christmas and End of Year Tax Phishing Scams," Northeastern University Information Services, December 2012.
11. "Symantec Intelligence Report," Symantec, January 2012.
12. "London Olympics: Stay Away from Scams, Data Theft, and Phishing," Zscaler, July 2012.
13. "Omniquad Warns Not to Fall for the London '2012 Olympic' Email Scam Fraudulently Evoking Both the Games and Their Sponsors," Omniquad, August 2012.

Phishing that Plays on Economic Fears

Today's economic turmoil offers unprecedented opportunities for criminals to exploit victims' fears. For instance, popular scams include emails that appear to be from a financial institution that recently acquired the target victim's bank, savings & loan, or mortgage holder.[14] In many cases, consumers are already unsure about the nature and status of these mergers and acquisitions, and phishers are eager to exploit that confusion.

The best defense against these scams is simple, clear, consistent communication with your customers at all stages of any business transition. The more they understand, the less likely they are to fall prey to the lures of a scammer.

Blended Phishing/Malware Threats

To increase success rates, some attacks combine phishing with malware for a blended attack model.[15] For instance, a potential victim receives a phishing e-card via email that appears to be legitimate. By clicking on the link inside the email to receive the card, the person is taken to a spoofed website which downloads a Trojan to the victim's computer. Alternatively, the victim may see a message that indicates a download of updated software is needed before the victim can view the card. When the victim downloads the software, it's actually a keylogger.

Phishing-based keyloggers use tracking components which attempt to monitor specific actions (and specific organizations such as financial institutions, online retailers, and e-commerce merchants) in order to obtain sensitive information such as account numbers, user IDs, and passwords.

Texting and Mobile Phone Phishing Scams

Posing as a real financial institution, phishers are using SMS (texting) as an alternative to email to gain access to confidential account information. These so-called "SMiShing" scams grew by 400 percent in the first half of 2012,[16] and in November researchers at North Carolina State University identified serious SMiShing vulnerabilities on multiple Android platforms.[17] (Once alerted, Google fixed the SMiShing bug within a matter of weeks.)

The typical scam informs the mobile phone user that the person's bank account has been compromised or credit card/ATM card has been deactivated. The potential victim is directed to call a number or go to a spoofed website to reactivate the card. Once on the site, or through an automated phone system, the potential victim is asked for card and account numbers and PIN numbers.

How Phishing Could Impact Your Business

While the financial industry continues to be a primary target for phishers, it's certainly not the only sector vulnerable to attack. Auction sites, payment services, retail, and social networking sites are also frequent targets, as are cell phone providers and manufacturers. In short, no business or brand is inherently safe.

Phishing attacks that pose as your company's official website diminish your online brand and deter customers from using your actual website out of fear of becoming fraud victims. In addition to the direct costs of fraud losses, other risks to your business include:

- A drop in online revenues and/or usage due to decreased customer trust
- Potential non-compliance fines if customer data is compromised

Even phishing scams aimed at other brands can impact your business. The resulting fear caused by phishing can cause consumers to stop making online transactions with anyone they can't trust.

Protecting Your Business

While there is no silver bullet, a number of technologies can help protect you and your customers. Many of the current phishing techniques rely on driving customers to spoofed websites to capture personal information. Technology such as Secure Sockets Layer (SSL) and Extended Validation (EV) SSL are critical in fighting phishing and other forms of cybercrime by encrypting sensitive information and authenticating your site.

Security best practices call for implementing the highest levels of encryption and authentication possible to protect against cyber fraud and build customer trust in the brand. SSL, the world standard for online security, is the technology used to encrypt and protect information transmitted over the Web with the ubiquitous HTTPS protocol. SSL protects data in motion, which can be intercepted and tampered with if sent unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware.

14. "FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A Phish-erman's Special," www.ftc.gov
15. "New Wave of Phishing Attacks Serves Malware to PCs and Macs," ZDNet, March 2012.
16. "How to Avoid Becoming a Victim of SMiShing (SMS Phishing)," Network World, March 2013.
17. "Smishing Vulnerability in Multiple Android Platforms (Including Gingerbread, Ice Cream Sandwich, and Jelly Bean)," NC State University, November 2012.

To help prevent phishing attacks from being successful and to build customer trust, you also need to show customers that you are a legitimate business. Extended Validation (EV) SSL Certificates are the answer, offering the highest level of authentication available with an SSL Certificate and tangible proof that the site is indeed legitimate.

EV SSL gives website visitors an easy and reliable way to establish trust online by triggering high-security browsers to display a green address bar with the name of the organization that owns the SSL Certificate and the name of the Certificate Authority that issued it.

The green bar demonstrates to site visitors that the transaction is encrypted and that your business has been authenticated according to the most rigorous industry standards. Cybercriminals cannot display their own name on the address bar, because the information shown there is outside of their control, and they cannot obtain a legitimate EV SSL Certificate due to the stringent authentication process. Extended Validation is simply beyond the power of phishers to exploit.

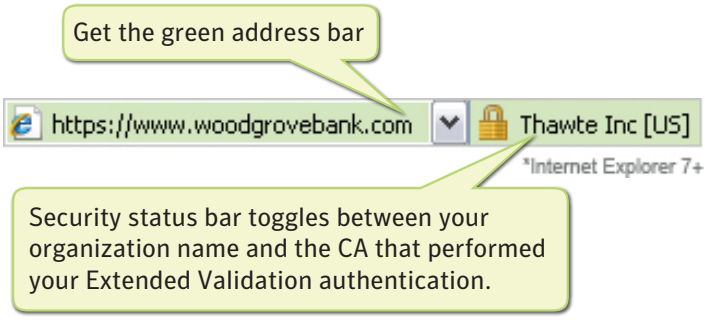

Figure 2. The green address bar triggered by an EV SSL Certificate, as it appears in Internet Explorer.

Consumer and Employee Education

In addition to implementing EV SSL technology, you should continue to educate your customers and employees on safe Internet practices and how to avoid cyber fraud. Teach them how to recognize the signs of a phishing attempt, including:

- Misspellings (less common as phishers become more sophisticated)
- Generic greetings instead of personalized, urgent calls to action
- Account status threats
- Requests for personal information
- Fake domain names/links

Also educate your customers and employees on how to recognize a valid, secure website before they provide any personal or sensitive information by:

- Looking for the green address bar
- Making sure the URL is HTTPS
- Clicking on the padlock to match the certificate information with the website they intend to visit

Education plays a key role in building trust. By helping customers validate their level of safety on your website, you can increase revenue, stand out from the competition, and even cut operational costs by moving more transactions online.

But always remember: phishers are tough, shape-shifting adversaries. Their scams will continue to evolve into new forms, while attempting to take advantage of human behaviors such as compassion, trust, or curiosity. Protecting your brand and your business from their malicious efforts will always require constant diligence. By embracing the latest SSL technologies, keeping up to date on the newest scams, and choosing a Certificate Authority with the highest possible standards for online security, you can stay one step ahead of phishers—and keep your business moving forward.

Glossary

Certificate Authority (CA) — A Certificate Authority is a trusted third-party organization that issues digital certificates such as Secure Sockets Layer (SSL) Certificates after verifying the information included in the Certificates.

Encryption — Encryption is the process of scrambling a message so that only the intended audience has access to the information. Secure Sockets Layer (SSL) technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive information from electronic eavesdropping.

Extended Validation (EV) SSL Certificate — Requires a high standard for verification of Secure Sockets (SSL) Certificates dictated by a third party, the CA/Browser Forum. In Microsoft® Internet Explorer and other popular high-security browsers, websites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

HTTPS — Web pages beginning with "https" instead of "http" enable secure information transmission via the protocol for secure http. "Https" is one measure of security to look for when sending or sharing confidential information such as credit card numbers, private data records, or business partner data.

Secure Sockets Layer (SSL) Technology — SSL and its successor, transport layer security (TLS), use cryptography to provide security for online transactions. SSL uses two keys to encrypt and decrypt data — a public key known to everyone and a private or secret key known only to the recipient of the message.

SSL Certificate — A Secure Sockets Layer (SSL) Certificate incorporates a digital signature to bind together a public key with an identity. SSL Certificates enable encryption of sensitive information during online transactions, and in the case of organizationally validated Certificates, also serve as an attestation of the Certificate owner's identity.

More Information

- **Via phone**
  - **US toll-free: +1 888 484 2983**
  - **UK: +44 203 450 5486**
  - **South Africa: +27 21 819 2800**
  - **Germany: +49 69 3807 89081**
  - **France: +33 1 57 32 42 68**
- **Email sales@thawte.com**
- **Visit our website at https://www.thawte.com/ssl**

Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first international specialist in online security. Backed by a 17-year track record of stability and reliability, a proven infrastructure, and world-class customer support, Thawte is the international partner of choice for businesses worldwide.