White paper

Phishing – The latest tactics and potential business impacts

Symantec™

Norton SECURED
powered by VeriSign

Phishing – The latest tactics and potential business impacts

Contents

Introduction

As one of the top cybercrime ploys impacting both consumers and businesses, phishing has remained a consistently potent threat over the past several years. In fact, there was an average of over 37,000 phishing attacks each month in 2012.[1]

You no longer need to be a sophisticated hacker to commit fraud on the Internet. Anyone who is motivated can join in, thanks to the off-the-shelf phishing kits provided by a thriving cybercrime ecosystem. Cybercriminals are even migrating to a new 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]

The impact on a business can be quite severe. RSA estimated in its February 2013 Fraud Report that worldwide losses reached $1.5 billion in 2012 and had the potential to reach over $2 billion if the average uptime of phishing attacks had remained the same as in 2011.[3] Whatever the threat – whether employees or customers have been phished, or the company website compromised – phishing is something to be taken very seriously. Organisations need to stay current on the latest methods employed by cybercriminals and take proactive steps to protect themselves from fraud.

This paper highlights the current growth and trends in today's phishing schemes, the potential impact on companies, and insight into how businesses can apply technology to protect themselves and their 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 a serious threat for both consumers and businesses. In the decade since phishing arrived on the scene, this fraud method has been growing rapidly, with one estimate citing approximately 8 million daily phishing attempts worldwide.[4] In 2012, one in every 414 emails transmitted over the web was related to phishing.[5]

The Anti-Phishing Working Group (APWG) reported in the second half of 2012 that there were 123,486 unique phishing attacks worldwide that involved 89,748 unique domain names, registering an increase of 32% in the number of attacks over the first half of 2012.[6] Although representing a larger number than the 115,472 attacks that the APWG observed in the first half of 2011, it was somewhat less than the record 126,697 observed in the second half of 2009, when the Avalanche botnet was on the loose.

Shared virtual server hacking explodes

Although hackers are always coming up with new phishing schemes, this one is actually an old – albeit obscure – one that has been successfully revived. In this attack, a phisher breaks into a web server that hosts large numbers of domains and places the phishing site content on every domain, so that every website on that server displays the phishing pages. In this manner, phishers can infect thousands of websites simultaneously. The APWG identified 42,448 unique attacks that used this strategy – a number representing 37 per cent of all phishing attacks globally.[7]

[1] 'RSA: February Fraud Report', RSA, February 2013.
[2] 'Verisign iDefense 2012 Cyber Threats and Trends', Verisign, 2012.
[3] 'RSA: February Fraud Report', RSA, February 2013.
[4] 'Counterfeiting & Spear Phishing – Growth Scams of 2009', Trade Me, Infonews.co.nz, March 2, 2009.
[5] Symantec 2013 Internet Threat Report, Symantec.com/threatreport
[6] 'Global Phishing Survey 2H2012: Trends and Domain Name Use', Anti-Phishing Working Group.
[7] Ibid.

Spammers continue to take advantage of holidays and global events

Each year in the run up to Christmas spammers spoof a number of legitimate retailers, offering Christmas 'deals' on a range of products. There were a large number of phishing campaigns relating to the Japanese earthquake, the 'Arab spring' movement and other notable global happenings. After the usual onslaught at Valentine's Day, anti-phishing experts expect to see similar scams around forthcoming marquee events.[8] Spear phishing attacks, although less in the news than in previous years, notably increase during holiday periods when businesses' security operations tend to be understaffed. That way, the cybercriminals' operations have a greater opportunity to succeed. However, this seems to be less the case between the Christmas and New Year's holidays. One possible explanation is that while security teams may be only lightly staffed, there are also significantly fewer employees working, therefore fewer opportunities for targeted users to open malicious attachments.

Phishing that plays on economic fears

Today's economic turmoil delivers unprecedented opportunities for criminals to exploit victims. For instance, popular scams include phishing emails that look like they are coming from a financial institution that recently acquired the target victim's bank, savings & loan or mortgage holder.[9] The large amount of merger and acquisition activity taking place creates an atmosphere of confusion for consumers, exacerbated by the dearth of consistent communications with customers. Phishers thrive in this type of situation.

Blended phishing/Malware threats

To increase success rates, some attacks combine phishing with malware for a blended attack model. 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 have tracking components which attempt to monitor specific actions (and specific organisations such as financial institutions, online retailers and e-commerce merchants) in order to obtain sensitive information such as account numbers, user IDs and passwords.

Another type of Trojan that enables phishers to capture sensitive information is a redirector. Redirectors route end users' network traffic to a location where it was not intended to go.

Man-in-the-middle SSL stripping

Back in 2008, a new type of malware was introduced that allows cybercriminals to spoof an encrypted session. This is a variance on the standard man-in-the-middle (MITM) attack that criminals use to access passwords or sensitive information passing unprotected over the network.

[8] 'Symantec Intelligence Report', Symantec, January 2012.
[9] 'FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A Phish-erman's Special', www.ftc.gov

Texting and mobile phone phishing scams
Posing as a real financial institution, phishers are using SMS as an alternative to email to attempt to gain access to confidential account information. Known as 'smishing,' 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 associated PIN numbers.

Spam and phishing move to social media
In the last few years, we have seen a significant increase in spam and phishing on social media sites. Criminals follow users to popular sites. As Facebook and Twitter have grown in popularity, they have also attracted more criminal activity. However, in the last year, online criminals have also started targeting newer, fast-growing sites such as Instagram, Pinterest, and Tumblr. Typical threats include fake gift cards and survey scams. These kinds of fake offer scams account for more than half (56 per cent) of all social media attacks.

How phishing could impact your business
While spam has declined slightly in 2012, phishing attacks have increased. Phishers are using very sophisticated fake websites – in some cases, perfect replicas of real sites – to trick victims into revealing personal information, passwords, credit card details and bank credentials. In the past they relied more on fake emails, but now those emails coupled with similar links posted on social media sites are used to lure the victim to these more advanced phishing websites. Typical fake sites include banks and credit card companies, as you'd expect, but also popular social media sites. The number of phishing sites that spoofed social network sites increased 123 per cent in 2012. If criminals can capture your social media login details, they can use your account to send phishing emails to all your friends. A message that seems to come from a friend appears much more trustworthy. Another way to use a cracked social media account is to send out a fake message to someone's friends about some kind of emergency.

In an attempt to bypass security and filtering software, criminals use complex website addresses and nested URL shortening services. They also use social engineering to motivate victims to click on links. In the last year, they have focused their messages around celebrities, movies, sports personalities and attractive gadgets such as smartphones and tablets.

Phishing attacks that pose as a company's official website diminish the company's online brand and deter customers from using the actual website out of fear of becoming a fraud victim. In addition to the direct costs of fraud losses, businesses whose customers fall victim to a phishing scam also risk:

- 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 a business. The resulting fear caused by phishing can cause consumers to stop transacting with anyone they can't trust.

Protecting your business

While there is no silver bullet, there are technologies that 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 helping customers authenticate 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 Web 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.

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

EV SSL gives website visitors an easy and reliable way to establish trust online by triggering high-security web browsers to display a green address bar with the name of the organisation that owns the SSL Certificate and the name of the Certificate Authority that issued it. Figure 1 shows the green address bar in Internet Explorer.

Figure 1. The green address bar triggered by an EV SSL Certificate.

The green bar shows site visitors that the transaction is encrypted and the organisation has been authenticated according to the most rigorous industry standard. Phishers can then no longer capitalise on visitors not noticing they are not on a true SSL session.

While cybercriminals are becoming adept at mimicking legitimate websites, without the company's EV SSL Certificate there is no way they can display its name on the address bar because the information shown there is outside of their control. And they cannot obtain the legitimate company's EV SSL Certificates because of the stringent authentication process.

Consumer and employee education

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

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

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

- Looking for the green bar
- Making sure the URL is HTTPS
- Clicking on the padlock to match the certificate information with the website they intended to go to
- Look for a trust seal such as the Norton Secured Seal

Education is a key component of building the trust necessary to overcome phishing fears. By helping your customers understand how to confirm they are safe on your website, you can grow revenues, differentiate your offering, and/or benefit from operational savings by moving more transactions online.

Phishers: Tough, shape-shifting cyber adversaries

Phishing will continue to evolve into new forms, while attempting to take advantage of human behaviours such as compassion, trust or curiosity. Protecting your brand and your business from phishing requires constant diligence, but pays rewards beyond reduced fraud losses.

By educating and protecting your customers with the highest levels of protection provided by EV SSL Certificates, your business can help ensure that customers have greater confidence in your online services. By demonstrating leadership in online security, you can broaden your market appeal and in doing so, generate new revenue streams.

For the most current information on global phishing trends, please visit the Symantec Monthly Intelligence Report.

Glossary

Certificate Authority (CA) — A Certificate Authority is a trusted third-party organisation 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 7 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 organisationally validated certificates, also serve as an attestation of the certificate owner's identity.

More Information

Visit our website

http://go.symantec.com/ssl-certificates

To speak with a product specialist

Call 0800 032 2101 or +44 (0) 20 8600 0740

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec (UK) Limited

350 Brook Drive, Green Park
Reading, Berkshire
RG2 6UH, United Kingdom
www.symantec.co.uk