DEFENDING AGAINST TODAY'S TARGETED PHISHING ATTACKS

websense®

Introduction

"Is this email a phish or is it legitimate?" That's the question that employees — and executives in particular — are asking with greater frequency. Is it hyper-paranoia or justified angst? Recent compromises — including those at a federal government laboratory, an email marketing giant, and a leading security technology organization — give credence to the latter, and evidence that hackers have adjusted their phishing attack tactics in ways that get past traditional email security defenses. In fact, although email remains highly vulnerable to foul play, security continues to rely heavily on principles and technologies that are more than a decade old. Organizations need to take a new look at email security, particularly as newer, more targeted phishing attacks proliferate.

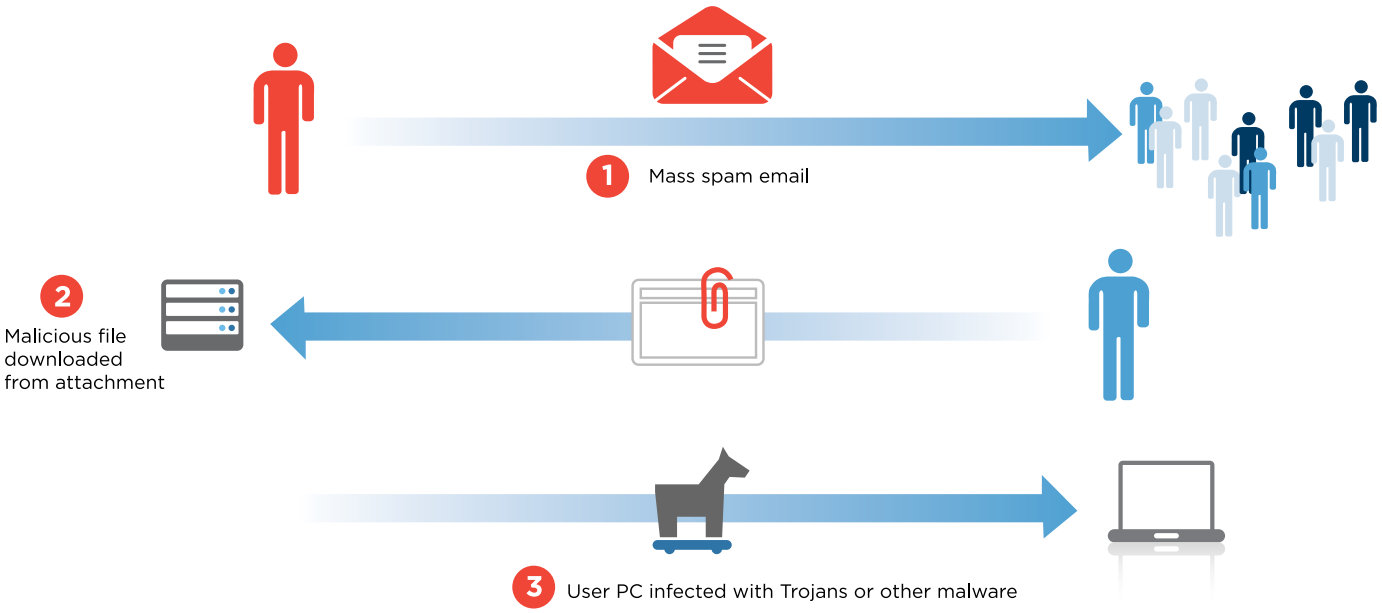
The Traditional Phishing Attack Model

Phishing attacks have long followed a tried-and-true model that relies upon a shotgun approach: high volumes of email, containing malware as an attachment or in the body of the email itself, are sent to untargeted recipients. The process is as follows:

1. **A hacker sends a mass email** to thousands of users.

2. **A small percentage of recipients act on the email** (e.g., downloading an attachment that contains a virus).

3. **The recipients' PC is infected with** a Trojan or other form of malware.



Traditional Defenses Against Phishing Attacks

Although the traditional phishing attack model has been effective for years, its efficacy has been waning. Users are now keen on recognizing and ignoring these attacks, having dealt with emails purporting to come from long-lost relatives in a faraway land for years.

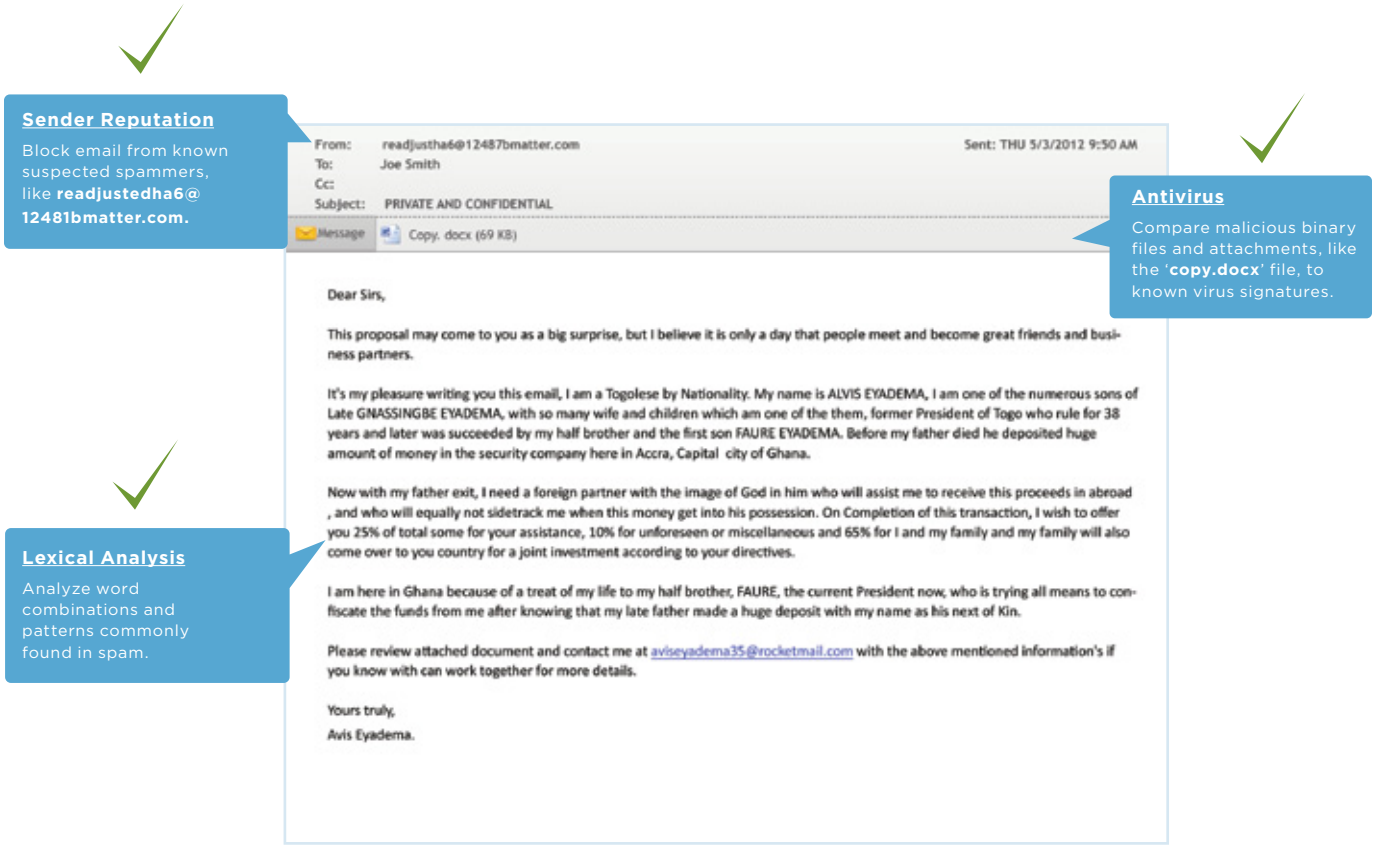
Traditional email security solutions, likewise, have become very proficient in sniffing out these schemes by employing technologies such as:

- **Sender Email Reputation** to identify addresses that are known to spew out spam.
- **Lexical Analysis** to analyze email content that contains word combinations and patterns commonly found in spam.
- **Antivirus** to help defend against known viruses that reside in email attachments.

These defense techniques have become so reliable and effective that many leading email security solutions now guarantee detection levels of 99 percent for all spam and 100 percent of all known viruses. As a result, most users no longer receive these emails in their inboxes.

The Evolution of Phishing Attacks

Though some hackers have been deterred by successful defenses, most have responded by modifying the phishing attack model in some slight yet significant ways. Though the basic framework remains in place, today's phishing attacks are lower in volume, highly targeted, and more legitimate in appearance. Moreover, malware is now delivered via an embedded URL.



The revised process is as follows:

1. Hackers target recipients by gathering intelligence on them from the likes of social networking websites.

2. Hackers compromise a legitimate domain or server, where targeted recipients may have an existing relationship, to gain access to a legitimate and therefore reputable email address.

3. Hackers use gathered intelligence to create phishing emails, which are sent via a reputable email address to targeted recipients.

4. A large percentage of recipients act on the email by clicking on an embedded URL that links to a legitimate but compromised website and surreptitiously downloads malware.

5. The malware looks for network vulnerabilities, perhaps to shut down security defenses and create back-door access to internal systems to capture valuable corporate information.

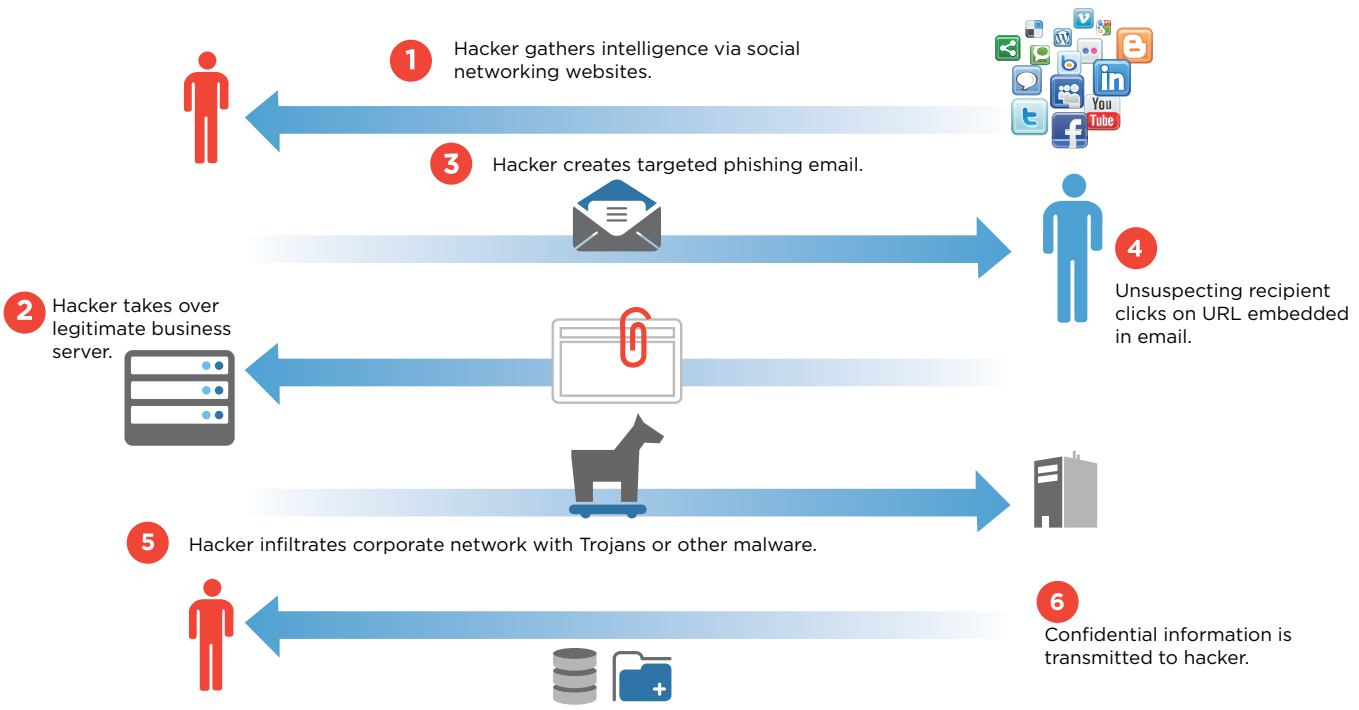
6. Confidential data such as intellectual property and customer data is stolen.

Why Traditional Defenses Fail

By just slightly modifying the traditional phishing attack model, hackers have hit pay dirt because they've been able to thwart traditional security measures:

- **Sender Email Reputation** fails to block the phishing email because it is sent from an address not traditionally associated with bulk or malicious emails.
- **Lexical Analysis** fails because the phishing email does not contain any word combinations commonly associated with spam.
- **Antivirus** fails because the malware isn't contained within the message but instead is delivered via a web page through obfuscated script.

The new phishing attack model has enabled hackers to compromise organizations such as Oak Ridge National Laboratory, known for its research into cyber security topics that include malware, vulnerabilities, and phishing. In an April 2011 attack,



57 of its users clicked on a malicious link that exploited a zero-day vulnerability within Internet Explorer (IE), exposing the individuals' Social Security numbers and birthdays. Similar attacks exposed sensitive information at the marketing giant Epsilon and at the security company RSA.

As low-volume, targeted phishing attacks proliferate, organizations need to reexamine their email security posture.

Best Practices to Catch Today's Phishing Attacks

As low-volume, targeted phishing attacks proliferate, organizations need to reexamine their email security posture. Here are a few starting points to help organizations adapt and minimize the risk of a compromise:

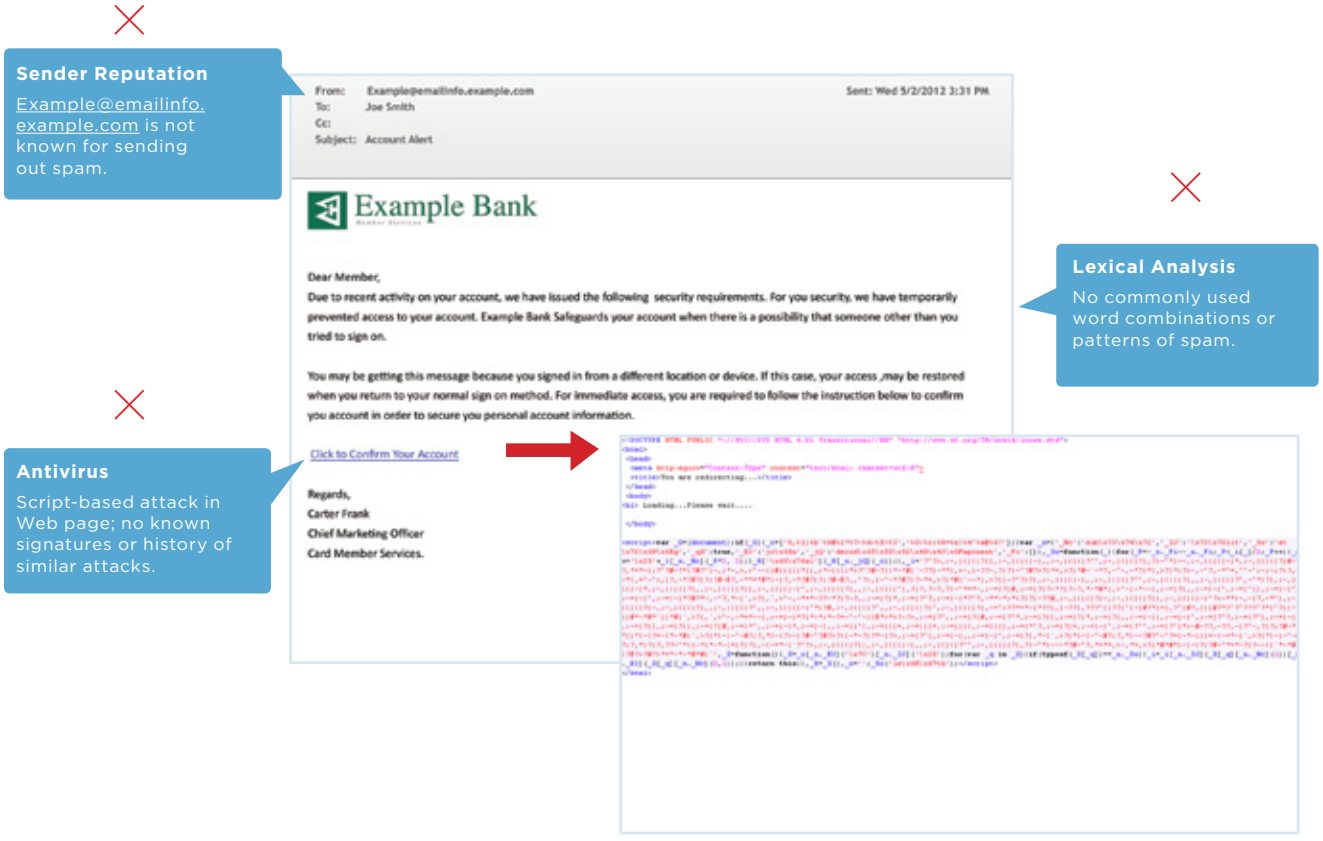
Web Intelligence Within Email Security Gateway

Almost all phishing attacks — 92 percent — now contain a web component to elude traditional email gateway antivirus defenses. URLs that are embedded in these emails often link to websites that are hosting obfuscated malware. Real-time web analytics and an up-to-date database of known good and malicious websites, including social networking sites, are vital to stop converged web and email threats from entering the inboxes of end-users.

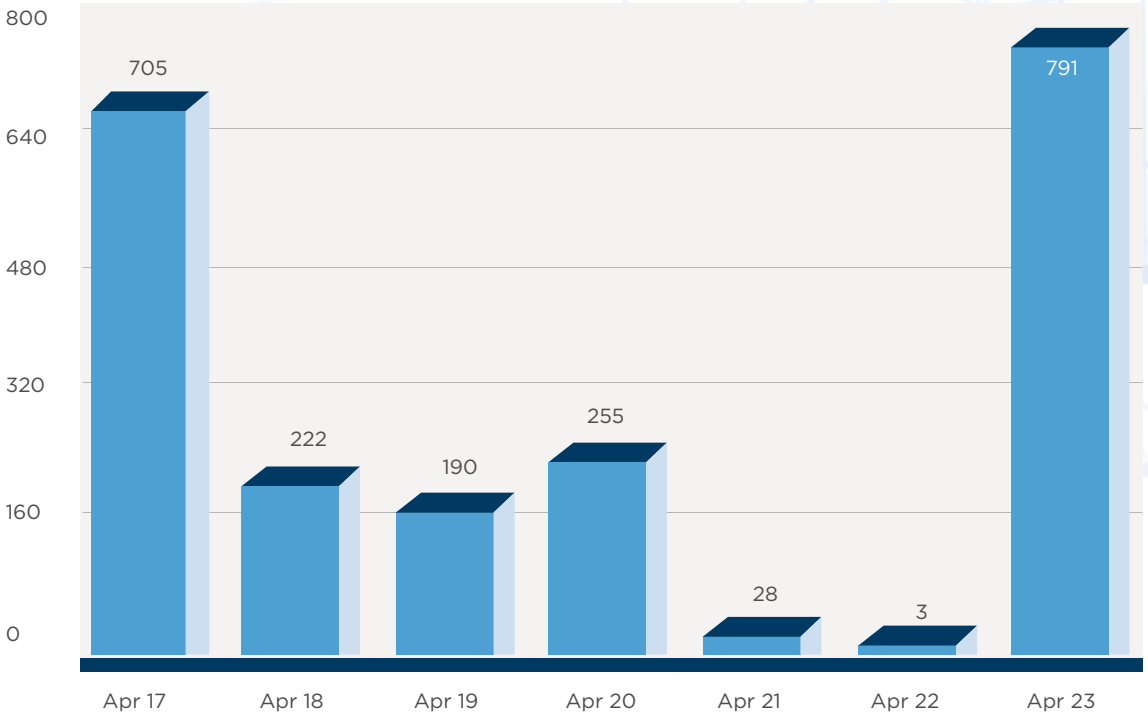
Recommendation: Combine gateway antivirus with proactive web threat intelligence in email security technology as part of a layered defense strategy.

Point-of-Click Threat Analysis

Modern phishing attacks succeed primarily because phishing emails now contain embedded links that point to dynamic-IP botnets or web pages that host dynamic code — two techniques that may elude even the most robust gateway malware analysis. For example, an email sent



Number of viruses detected by Websense Advanced Detection NOT detected by 5 top antivirus engines (Apr 17- Apr 23).



at midnight may contain a link to a web page that was harmless on the initial security scan at the gateway. However, the same web page may include injected malicious code when the recipient clicks on the link the following morning. Every week, an average of more than 700 pieces of malware is delivered using this attack model — undetected by the leading antivirus engines.

Recommendation: Isolate and sandbox suspicious emails that contain URLs for real-time analysis at point-of-recipient-click to reduce security risk while not increasing false positives or compromising end-user experience.

Real-Time Analysis of Data Transmission

Modern hackers are after data, and not just any data. They seek intellectual property, product roadmaps, and anything that might be of vital importance to business success. Organizations need an extra line of defense in their email infrastructure, and in the data-accessing devices such as tablets and smartphones, to oversee the flow of information and prevent data loss.

Recommendation: Analyze all outbound data to automatically block, quarantine, or encrypt sensitive data, and monitor for patterns that may indicate a slow but steady leak of important information.

Immersive End-User Training

Installing the latest security solutions means nothing if users don't practice cyber safety. Remember that the wall between a user's personal life and work life has shrunk or fallen altogether. That means users can be well protected at work, but not when checking personal email on their company-issued laptop at home. The best way to get them to "think security" is to raise awareness within the organization of the strategies and tactics used by today's hackers.

Recommendation: Immerse employees with examples of real-world phishing attacks, allowing for the opportunity to relay immediate, focused feedback and training to those who fall victim to the exercises.