proofpoint.

THE DEFINITIVE EMAIL SECURITY STRATEGY GUIDE

TABLE OF CONTENTS

INTRODUCTION

EMAIL IS A TOP THREAT VECTOR

Data breaches have become one of today's biggest business threats. In the U.S. alone, companies and government agencies suffered a record 1,093 data breaches last year. That's a 40% increase from the year before, according to the Identify Theft Resource Center. [1]

The top threat vector for those data breaches: email. According to Verizon, email fraud accounts for 95% of enterprise attacks.[2]

Email threats are versatile and are growing faster than ever. To fight back, organizations must invest in an end-to-end email security strategy that addresses the entire email attack chain—from proactive prevention through real-time threat response.

This guide will help you do just that.

95%

of enterprise attacks are email fraud

[1] Identity Theft Resource Center. " ITRC Data Breach Report 2016." January 2017.

[2] Verizon. "2016 Data Breach Investigations Report." April 2016

TODAY'S EMAIL SECURITY TOOLS ARE FAILING

There's a 22% chance that any given organization will experience a data breach of at least 10,000 records within the next 24 hours.

Source: Proofpoint

Only 31% of companies have a budget in place for data breach mitigation.

Source: Osterman Research

75% of organizations would take hours, days or weeks to detect a breach.

Source: Osterman Research

THE PROBLEM

ATTACKS ARE EVOLVING FASTER THAN EMAIL DEFENSES

Since its inception, email has been a favorite target for cyber criminals hoping to steal sensitive data, user credentials, and company funds. In response, organizations have deployed a wide range of email security tools. Most of these focused on protecting the network.

But attack techniques are evolving fast. Solutions built for fighting the attacks of two to three years ago are struggling to keep up. For example, business email compromise (BEC) email fraud was barely on the radar 24 months ago. Now, it has eclipsed ransomware in terms of monetary loss. Ransomware, in turn, continues to adapt and flourish—39% of organizations were hit with ransomware in 2016, according to Osterman Research.[3]

Amid dramatic headlines and more aggressive regulation, organizations are expected to spend more than $90 billion on cybersecurity in 2018. And still, email attacks are more effective today than ever. According to Verizon, 30% of recipients open phishing messages, and 12% go on to click malicious attachments.[4]

That's a huge disconnect. Organizations are spending more on cybersecurity than ever, even as losses from data breaches, business disruption and fraud continue to mount. The divide stems from misconceptions about where threats come from and how they work. Before we can proactively fight today's email threats and prevent the data breaches that result from them, we must better understand them.

[3] Osterman Research. "The State of Ransomware." August 2016.

[4] Verizon. "2016 Data Breach Investigations Report." April 2016.

TODAY'S TOP EMAIL FRAUD TACTICS

Cyber criminals use a wide range of tactics to launch email attacks. Chief among them are BEC, advanced malware, and outbound phishing.

BUSINESS EMAIL COMPROMISE (BEC)

BEC attacks are difficult for traditional email security tools to catch. That's because they are sent in low volumes. There's usually no payload to sandbox, no URL to check, no reputation to look up. These attacks target your employees using manipulation alone. A fraudulent email appearing to come from the CEO asks your CFO to wire money. Your finance manager receives new account information from what seems to be a legitimate vendor. Someone in the human resources office gets a request from her "boss" for employee records.

WHAT IS BEC?

BEC email attacks are also known as impostor email and CEO fraud. They're highly-targeted, low volume email attacks that impersonate corporate identities to solicit fraudulent wire transfers, steal company data, access customer credentials and get other confidential information.

BEC

Here are the top BEC techniques:

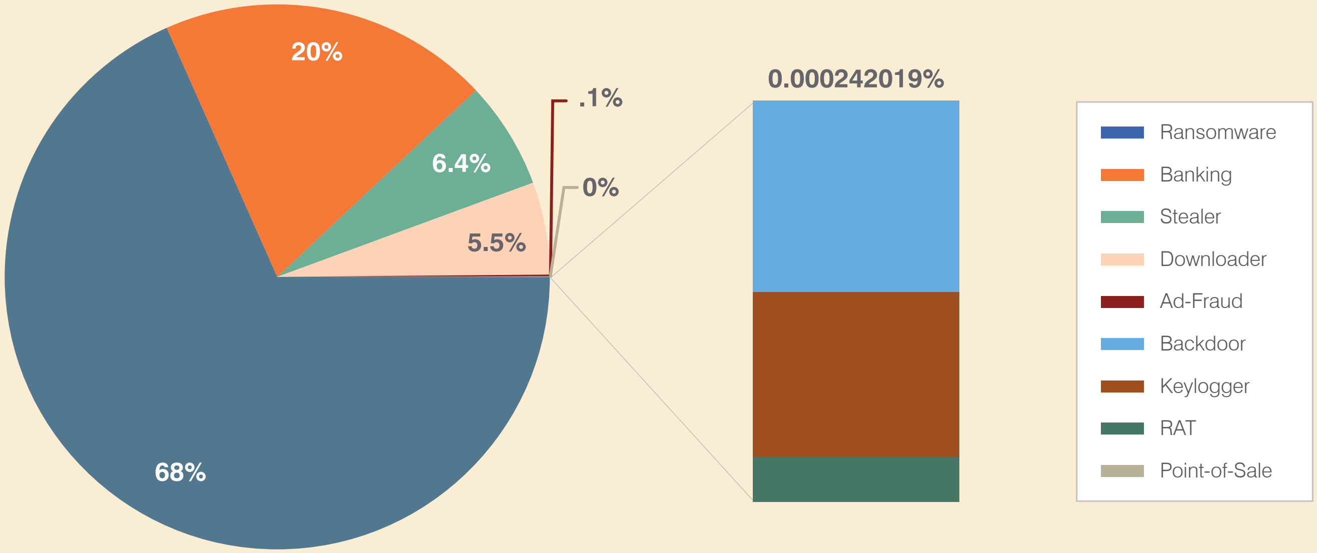
1. Spoofing Email Fields

Spoofing email fields is a popular BEC tactic. Attackers have several ways of doing this, including:

- Changing the reply-to email address in a way that makes it look like the email is coming from within the organization
- Spoofing the display name (which is especially effective on mobile devices that hide the reply-to email address)
- Using use a domain that looks like the company's but is slightly different (such as using a numeral zero in place of the letter 'o')
- Pretending to be a legitimate business partner or supplier.

BEC TECHNIQUES AT A GLANCE

MALWARE BY CATEGORY, Q1 2017

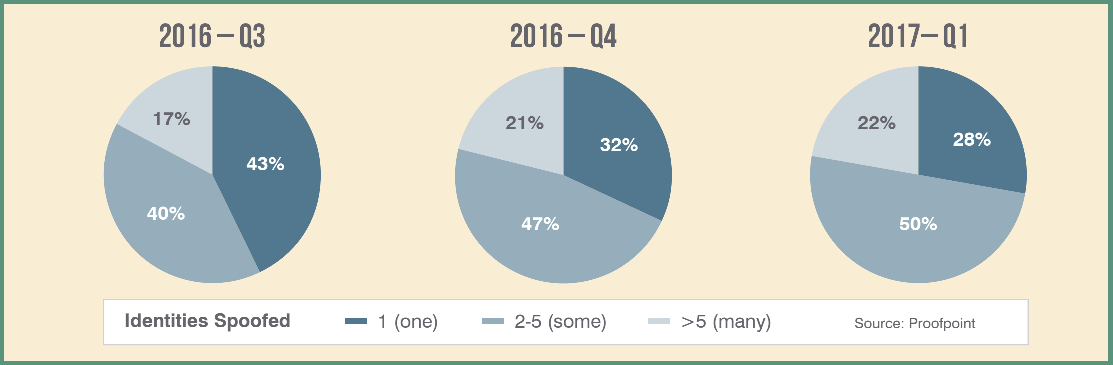


Source: Proofpoint

Comparison of quarterly overall message volume

2. Targeting a Range of Employees

When BEC scams first appeared, cyber criminals usually focused on targeting the CEO/CFO relationship. Now more BEC scams spoof other identities. And the number of people being targeted within organizations is up, rising 50% from Q3 2016 to Q1 2017 alone.



Source: Proofpoint

3. Getting Creative with Subject Lines

Using “clickbait” subject lines is another favorite BEC tactic. Urgent language is the most popular—employees are more likely to pay attention to a fraudulent reply-to address if the subject line suggests that someone in authority needs something from them. Here’s a look at the most popular BEC subject lines our researchers discovered in the first quarter of 2017:

MOST POPULAR BEC SUBJECT LINES

20%	=	Request
17%	=	Urgent
7%	=	Bank
2%	=	FYI

Instead of using just one BEC technique, cyber criminals use all of them. When one doesn’t work, they’ll go down the list until someone responds. That’s why you need to implement a multi-layered BEC solution that can fight the full range of threats.

ADVANCED MALWARE

Unlike BEC, which is new, advanced malware attacks have been around for a long time. And over the last few years, the number of ransomware variants has multiplied so much that many traditional defenses can't stop them all.

Take sandboxing. Sandboxes work by running suspect code from attachments and URLs in a virtual environment to see what it does if someone clicks. A sandboxing tool that may have worked last year would have to work 30 times faster today to keep up with the size and scale of this year's ransomware threats. And it would have to adapt to every new sandbox-evasion technique developed in that timeframe.

To fight back, you need a security solution that can keep up with the speed, scale and agility of these evolving ransomware attacks.

WHAT IS ADVANCED MALWARE?

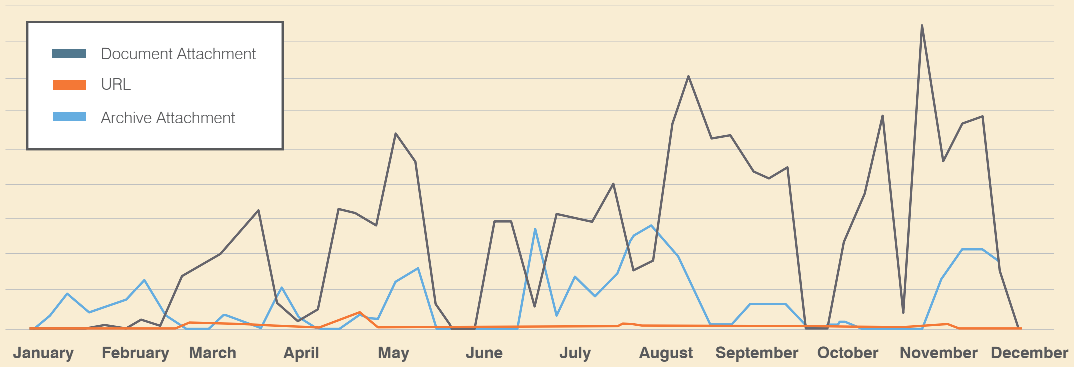
Advanced malware threats are delivered through malicious email attachments and URLs. They include ransomware, polymorphic malware, zero-day exploits and weaponized documents that exploit technical flaws in popular business software.

Malicious document attachment messages increased 600% in 2016
Source: Proofpoint

Messages distributing ransomware accounted forever 80% of total malicious message volume
Source: Proofpoint

The number of ransomware variants multiplied 30 times over last year
Source: Proofpoint

Indexed Weekly Malicious Message Volume by Attack Type, 2016



Source: Proofpoint

OUTBOUND PHISHING

When it comes to email security, we usually don’t consider our outbound phishing risk. We’re more concerned with protecting our employees and network by securing email coming into the organization and protecting our confidential data by monitoring and encrypting email going out of the organization.

But cyber criminals quietly spoofing your brand outside of your email gateway can hurt your reputation—and bottom line. These sophisticated phishing attacks are hard to spot, especially as consumers embrace new digital tools. More than half of all email is already opened on a mobile device.[5]

The figure to the right shows two outbound phishing examples.

The first example (left) spoofs a legitimate Wells Fargo domain (onlinebanking@alerts.wellsfargo.com). The other uses an unrelated domain in a way that makes it appear related to PayPal (paypal@service.com).

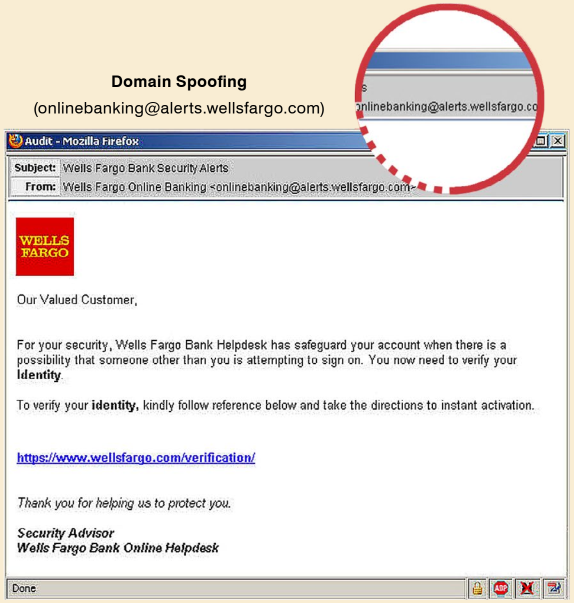
WHAT IS OUTBOUND PHISHING?

Outbound phishing attacks spoof corporate and/or brand identities to solicit data, money and other confidential information from customers and suppliers.

BRAND PHISHING SCHEME

Domain Spoofing

(onlinebanking@alerts.wellsfargo.com)



Audit - Mozilla Firefox

Subject: Wells Fargo Bank Security Alerts

From: Wells Fargo Online Banking <onlinebanking@alerts.wellsfargo.com>

WELLS FARGO

Our Valued Customer,

For your security, Wells Fargo Bank Helpdesk has safeguard your account when there is a possibility that someone other than you is attempting to sign on. You now need to verify your **Identity**.

To verify your **identity,** kindly follow reference below and take the directions to instant activation.

https://www.wellsfargo.com/verification/

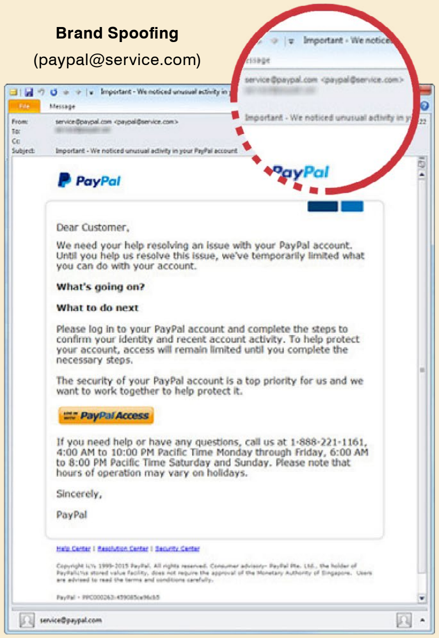
Thank you for helping us to protect you.

Security Advisor
Wells Fargo Bank Online Helpdesk

Done

Brand Spoofing

(paypal@service.com)



Important - We noticed unusual activity in y

File Message

From: service@paypal.com <paypal@service.com>

To:

Cc:

Subject: Important - We noticed unusual activity in your PayPal account

PayPal

Dear Customer,

We need your help resolving an issue with your PayPal account. Until you help us resolve this issue, we've temporarily limited what you can do with your account.

What's going on?

What to do next

Please log in to your PayPal account and complete the steps to confirm your identity and recent account activity. To help protect your account, access will remain limited until you complete the necessary steps.

The security of your PayPal account is a top priority for us and we want to work together to help protect it.

PayPal Access

If you need help or have any questions, call us at 1-888-221-1161, 4:00 AM to 10:00 PM Pacific Time Monday through Friday, 6:00 AM to 8:00 PM Pacific Time Saturday and Sunday. Please note that hours of operation may vary on holidays.

Sincerely,

PayPal

Help Center | Resolution Center | Security Center

Copyright © 1999-2015 PayPal. All rights reserved. Consumer advisory- PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.

PayPal - PPC000263:459085ca96cb5

service@paypal.com

[5] Lauren Smith (Litmus). “February 2016 Email Market Share: Mobile Opens Climb Back to 55%.” March 2016.

Outbound phishing might not seem much of a threat because it doesn't directly target your employees or infect your systems. But it can be a huge problem for your business.

Phishing tarnished your organization's reputation. After being phished or spoofed by an impostor, customers are 42% less likely to interact with your brand.

According to a study conducted by Return Path, outbound phishing also damages the deliverability and performance of your legitimate marketing emails:

One in five phishing attacks negatively impacts the deliverability of a brand's marketing emails

When negatively affected, the average inbox placement rate drops by up to **10 percentage points** at Gmail.

When negatively affected, the average inbox placement rate drops by up to **7 percentage points** at Yahoo.

One in three phishing attacks results in reduced subscriber engagements.

When negatively affected, the average read rate drops by up to **18 percentage points** at Gmail.

When negatively affected, the average read rate drops by up to **11 percentage points** at Yahoo.

Even though these outbound phishing emails occur outside of your gateway, your customers make purchase decisions based on their impact. Identifying who is using your brand name over email is critical.

Unfortunately, there is no single way to fight the diverse range of threats facing your organization. No matter how sophisticated your email security, some threats will inevitably get through.

Your best defense is a multi-layered one that offers protection at every stage of the attack chain, securing emails that come in, protecting data that goes out, and responding to threats in real time.

THE VALUE OF BRAND TRUST

57%

of the purchase decision is already made by a B2B buyer before they engaged with sales.

Source: Harvard Business Review

$

5%

increase in customer retention can lead to a 25-95% increase in company profits

Source: Harvard Business Review

88%

of marketers believe that brand trust influences revenue.

Source: Return Path Survey

FIVE STEPS TO BUILDING YOUR EMAIL SECURITY STRATEGY

STEP 1: VISIBILITY

To defend your organization effectively from email attacks, you must understand the threats you face. Robust threat intelligence that can detect the full scale of malicious emails is an important first step, but it’s not enough. You must also implement a solution that can correlate and analyze your threat data, revealing who is being targeted, who is attacking you and what information they are trying to steal. When you have an accurate threat analysis, you can better identify the steps you need to take to fight back.

STEP 2: DEPLOY CORE EMAIL CONTROL AND CONTENT ANALYSIS

Maintaining control over what messages get into your environment is critical when it comes to email security. Your solution must offer granular classification that doesn't just look for spam or malware but also identifies all distinct types of email (malicious or not) targeting your employees.

These emails could include bulk mail, credential phishing, BEC attacks, adult content, and more. Your classification tool should include advanced sandboxing capabilities that can analyze every attachment and URL in real time as it comes into your gateway.

Being able to customize email policies is another important feature of your control system. If you empower employees to choose how they want to handle bulk mail, they may be able to spot malicious content more easily.

STEP 3: AUTHENTICATE YOUR EMAIL

Protecting the email gateway is essential. But as we explored above, outbound phishing emails targeting customers and partners outside of the gateway pose serious risks to your business as well. Email authentication, specifically DMARC (Domain-based Message Authentication Reporting and Conformance), is the solution to threats like these.

DMARC ensures that legitimate email is properly authenticating against established SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) standards. It blocks any fraudulent activity from domains under your organization's control (such as active sending domains, non-sending domains, and defensively registered domains).

Authenticating your email will reveal who is sending email on your behalf. That insight empowers you to block threats targeting your customers and partners and protect your brand's reputation.

DMARC ENSURES THAT LEGITIMATE EMAIL IS PROPERLY AUTHENTICATING—AND THAT FRAUDULENT ACTIVITY APPEARING TO COME FROM YOUR ORGANIZATION'S DOMAINS IS BLOCKED

YOUR RESPONSE SOLUTION SHOULD BE ABLE TO

Remove and analyze all malicious emails from inboxes

Enable email continuity in the event of an email server going down

Correlate email threats with your wider network (firewalls, endpoints, IDS, IPS) to help you gain wider visibility

STEP 4: PREVENT DATA LOSS

There's a lot we can do to stop threats from coming in. But you should also prevent sensitive data from leaving your gateway. An effective email security strategy prepares for any threats that make it through your defenses—and employees who inadvertently expose sensitive data. Your solution should combine encryption with data loss prevention (DLP) so that sensitive information, even if exposed or exfiltrated, is always protected.

STEP 5: RESPOND TO THREATS IN REAL TIME

No security solution can stop all attacks. Real-time threat response must be a pillar of your email security strategy.

Be wary of any email security vendor that claims to catch every threat. If such a solution were on the market today, data breaches and email fraud would be a thing of the past. As recent headlines prove, this is simply not the case.

GETTING STARTED

Your best defense is understanding and preparation. Know the threats targeting your organization, identify your weak spots, and craft an email security defense that offers protection across these five key areas of the email threat lifecycle: visibility, content control and analysis, authentication, data loss prevention, and response.

Request an email threat assessment to uncover your email risk exposure and current vulnerabilities. Visit www.proofpoint.com/email-assessment

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.