

CALYPTIX SECURITY

# Email Phishing for IT Providers

*How phishing emails have changed and how to protect your IT clients*



**calyptix**<sup>®</sup>  
SECURITY

(800) 650-8930 | [info@calyptix.com](mailto:info@calyptix.com)

# Contents

<i>Introduction</i> .....	2
<i>Phishing overview</i> .....	3
<i>Trends in phishing emails</i> .....	6
<i>Email phishing tactics</i> .....	11
<i>Steps for MSP &amp; VARS</i> .....	24
<i>Advice for your clients</i> .....	29
<i>Sources</i> .....	35

# Introduction

There are only so many ways to break into a bank. You can march through the door. You can climb through a window. You can tunnel through the floor. There is the service entrance, the employee entrance, and access on the roof.

Criminals who want to rob a bank will probably use an open route – such as a side door. It's easier than breaking down a wall.

Criminals who want to break into your network face a similar challenge. They need to enter. They can look for a weakness in your network – maybe a vulnerability in your server – but it's easier for them to use an open route. Email is one of their favorites.

Email is a door into your network. Data passes through it every day. If criminals want to break in, some will throw on a disguise and try to sneak by. By pretending to be someone else, such as someone you respect, they will try to earn enough of your trust to steal from you.



This is called **Phishing**

Phishing is the practice of pretending to be a trusted entity with the goal of stealing someone's information. The most common type is email phishing, and that is the focus of this report.

# Overview

## What is phishing?

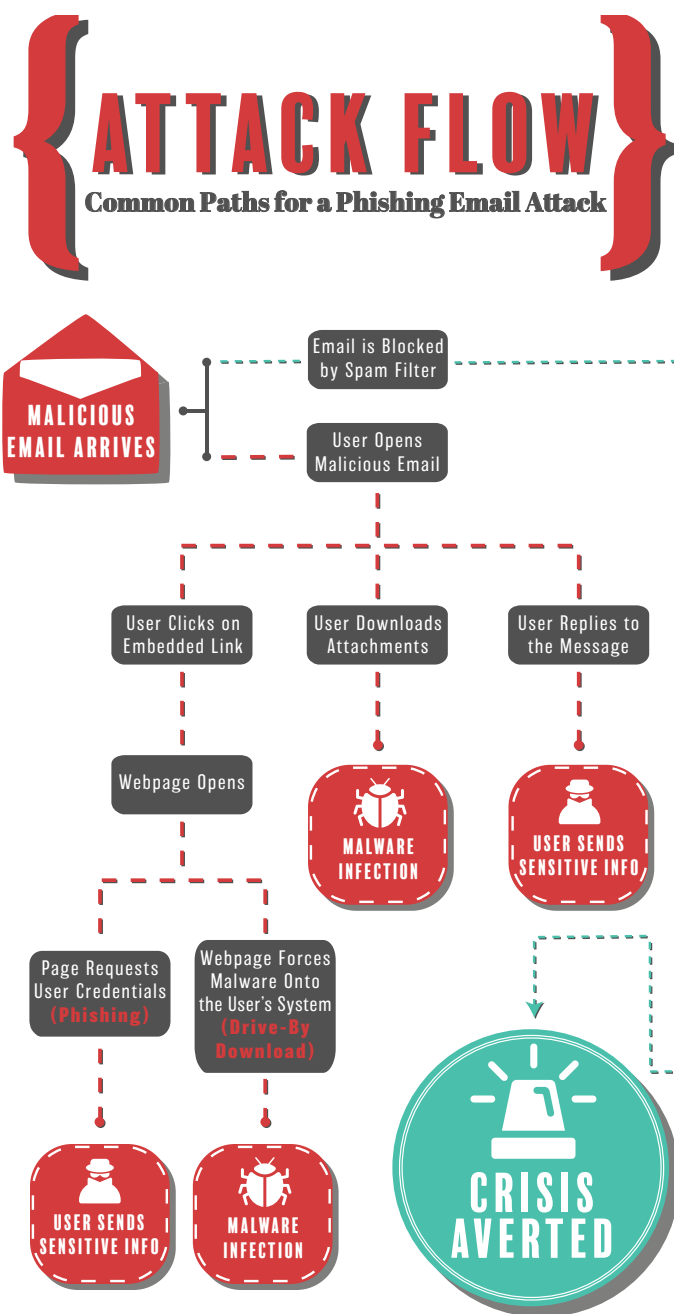
Email phishing works like this:

1. A criminal sends an email to a potential victim. The email appears to come from a trusted sender – such as a bank or one of the victim's contacts.
2. The email urges the person to download an attachment, click a link, or reply to the message with sensitive information.
3. The person either disregards the email or takes the action requested by the sender. If the action is taken, then the person is one step closer to becoming a victim.

Many phishing emails are the beginning of a larger attack, such as the theft of a customer database. For example, by successfully phishing a victim's administrative credentials, an attacker may identify several servers and databases on the network, breach them, and export the data.

**Author's Note:** This report defines phishing emails as a sub-type of malicious email that are designed to extract information from a target. Other reports use a broader definition that includes other types of malicious email, such as messages that infect victims with ransomware.

Since these types do not have a primary goal of extracting information from users, we consider them outside the scope of this report. However, many of the suggestions we provide can apply to all types of malicious email.



# Overview

## *Big data breaches are phishy*

Email phishing has been around since the 1980s. With roughly 30 years to work on the problem, you might suspect a security expert had solved it. That's not the case.

Email phishing is one of the most popular means of launching a cyber attack. It's found worldwide across all industries and company sizes.

Some of the most well-known cyber attacks in the last five years began with clever phishing emails.

### **Target Corp – Nov. 2013**

Attackers successfully phished an HVAC company that subcontracted with Target. This led to the breach of Target's network and the theft of 110 million customer and credit card records.


### **Sony Corp – Fall 2014**

Company executives gave up their Apple ID credentials in response to a spear phishing campaign. This led to the crippling of the company's network and mass destruction of its data. Before deleting the data, the attackers published much of it online. This included unfinished movie scripts, salary lists, thousands of social security numbers, and thousands of company emails.

### **Anthem – Jan. 2015**

Investigators suspect the breach of Anthem, the second-largest health insurance provider in the U.S., began with phishing emails. The messages tricked several employees into visiting fake websites controlled by the attackers and entering their login credentials. The breach compromised the personal information of about 80 million people, or the rough equivalent of 25% of the U.S. population.

As you will see later in this report, all trends indicate that email phishing is here to stay, and in many ways the problem is getting worse.



**95% of all attacks on**  
*enterprise networks are*  
*the result of* **successful**  
**spear phishing.**

***Alan Paller, SANS Research Director  
via Network World***

# Overview

## *Small businesses are a phishing pond*

Data breaches at huge corporations make great headlines, but they obscure an important fact: small and medium businesses (SMBs) are major targets for spear phishing attacks.

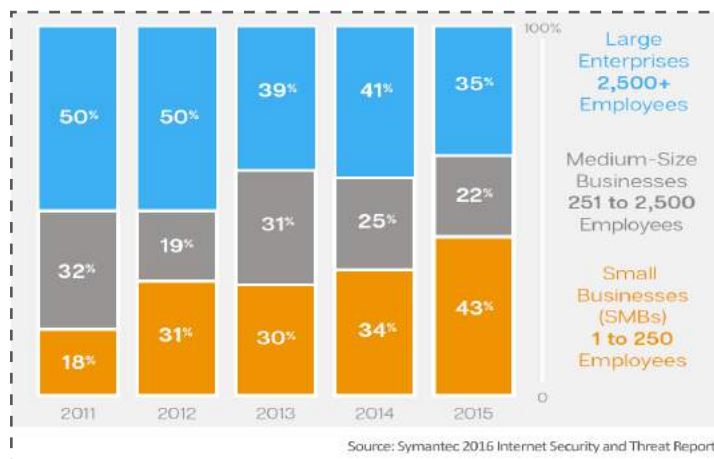
Spear phishing is nearly identical to standard email phishing – except it is more targeted. Rather than sending the same message to millions of addresses, the attackers focus on a specific person or group.

Targets of spear phishing can be as broad as “all accountants at businesses with 100 or fewer employees.” Or it can be as narrow as “Jennifer Johnson the CPA at Acme Inc.” By researching the target and tailoring their emails and tactics, the attackers greatly improve their success rate. (More about spear phishing in the next section)

The proportion of spear phishing attacks against SMBs has grown every year since 2013. Last year, 43% of all spear phishing attacks targeted companies with fewer than 250 employees, according to this chart from the Symantec 2016 Internet Security Threat Report (ISTR).

Small businesses may not make headlines when they are hit by a phishing attack, but the results can be devastating nonetheless. Data theft, financial loss, and tarnished reputations are just the beginning of a long road that victims can be forced to march.

## *Spear-Phishing Attacks by Size of Targeted Organization*



# Trends in Phishing Emails

## 1. Custom emails with fewer targets

Phishing attackers used a batch-and-blast approach for years. They crafted campaigns on a mass scale. One phishing email was sent to thousands – even millions – of people with the hope of a success rate in the low single digits.

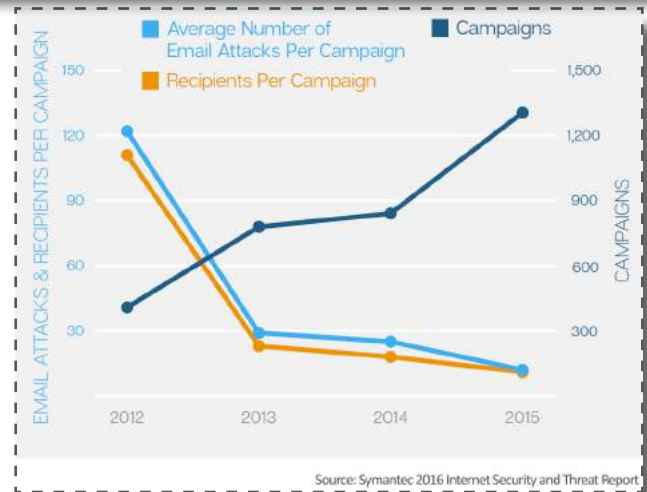
Today, mass phishing is still popular, but it is in decline. Cyber criminals have grown savvier and are investing in custom attacks against smaller groups (i.e. spear phishing).

Data across the industry conflicts on this issue, but a chart from the 2016 ISTR fits the consensus: attackers are sending fewer emails to smaller lists, but the number of phishing campaigns and their impact have jumped.

As any email marketer will tell you, a custom email sent to a smaller list will often outperform a generic email sent to a massive list. Criminals are beginning to understand this principle.

A custom email can include more details that resonate with recipients and earn more trust, thereby making people more like to “convert.” The main difference is that marketers want to convert you into a buyer and criminals want to convert you into a victim.

### Spear-Phishing Email Campaigns



# Trends in Phishing Emails

## 2. Higher infection rates

Phishing tactics have improved greatly from the Nigerian prince emails of the 1990s. The emails can be very convincing.

Nearly one-third of all phishing messages reviewed for the Verizon 2016 Data Breach Investigations Report (DBIR) were opened, and a terrifying 12% were clicked. This represents a big jump in open rate for phishing emails compared to previous years, and a slight rise in the click rate.

This suggests that phishing emails are improving in sophistication. The attackers are sharpening their skills to persuade more people to open the message and click the link or attachment.

“The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds.” Verizon 2016 DBIR.

Malicious emails can also be difficult to spot. Attackers constantly change tactics to avoid detection by humans and spam filters.

In a quiz that tested the ability of business users to detect phishing emails, only 6% of respondents (out of more than 50,000) could identify all of the malicious messages. On average, they identified only 35% of the bad emails, according to McAfee’s report, Phishing Deceives the Masses.

**In short:** phishing emails can be very effective and their tactics are improving.

← ----- ● -----  
“The **median time** for the **first user** of a phishing campaign to **open** the malicious email is **1 minute, 40 seconds.**”

Verizon 2016 DBIR

----- > ----- ●

# Trends in Phishing Emails

## 3. Attackers want credentials

Most phishing attempts are laser-focused on stealing login credentials, such as the victim's username and password for online banking or internal systems. This is made clear in the chart to the right from the 2016 DBIR.

While 90% of phishers want to sink a hook into a victim's login credentials, about 7% want to steal secrets, such as trade secrets in the manufacturing industry.

The 90:10 ratio is also reflected in the attackers' motivations. Nine out of 10 phishing attacks are launched by organized crime and most of the rest are launched by state-sponsored attackers, according to the 2016 DBIR.

This makes sense, since organized crime syndicates are often looking for login credentials to either directly access bank accounts or steal personal data that can be sold or used for identity theft.

State-affiliated actors are less likely to be interested in a person's credit card number and are likely more interested in how a target company makes a superior product.

### Top Five Data Varieties Breached by Phishing Attacks (n=905)



**“Main perpetrators of phishing attacks are organized crime syndicates (89%) and state-affiliated actors (9%).”**

**Verizon 2016 DBIR**

# Trends in Phishing Emails

## 4. Retailers hit by broad attacks

### Phishing Ratio in Email by Industry

Industry Detail	Phish Email Ratio
Retail Trade	1 in 690
Public Administration	1 in 1,198
Agriculture, Forestry, & Fishing	1 in 1,229
Nonclassifiable Establishments	1 in 1,708
Services	1 in 1,717
Manufacturing	1 in 1,999
Finance, Insurance, & Real Estate	1 in 2,200
Mining	1 in 2,225
Wholesale Trade	1 in 2,226
Construction	1 in 2,349
Transportation & Public Utilities	1 in 2,948
Non SIC Related Industries	
Energy	1 in 2,525
Healthcare	1 in 2,711

Source: Symantec 2016 Internet Security and Threat Report

No industry is safe from cyber attacks. And since phishing is such a prevalent part of cyber crime, it follows that no industry is immune to phishing.

Some industries are natural targets and receive more attacks. The retail sector, which processes huge volumes of personal and credit card data, is the largest target.

About 1 in every 690 emails received by a retail company is a phishing attempt. This is almost twice the rate of phishing emails as the second most targeted industry, public administration, according to the chart to the left from the 2016 ISTR.

# Trends in Phishing Emails

## 5. Banks hit by targeted attacks

Retail may be the biggest target for general phishing attacks, but when it comes to spear phishing, the prime targets are the industries that deal with big money – the finance, insurance, and real estate companies.

Comparing the two previous charts suggests that the criminals behind these attacks are similar to businesses. They want to maximize their return on investment, only they invest in crime instead of products and capital.

For example, in the financial industry, a successful phishing attack can open a bank account. This allows attackers to directly wire money into accounts they control. Once the breach occurs, the payoff can be very large and very fast. Therefore, attackers are willing to invest more time and effort into a narrow spear phishing campaign against a bank because a single breach can net a massive profit.

Attacks in the retail industry are likely less profitable. Often netting credit card and personal data, which is typically sold on the black market or used for identity theft, these attacks take longer to payoff and generate less money on average. Therefore, attackers may have to successfully breach more targets to earn a healthy profit. They need more victims to earn good returns, so they invest in broad campaigns that require generic messages.

### Top Industries Targeted by Spear-Phishing Attacks

Industry Detail	Distribution	Attacks per Org	% Risk in Group*
Finance, Insurance, & Real Estate	35%	4.1	8.7%
Services	22%	2.1	2.5%
Manufacturing	14%	1.8	8.0%
Transportation & Public Utilities	13%	2.7	10.7%
Wholesale Trade	9%	1.9	6.9%
Retail Trade	3%	2.1	2.4%
Public Administration	2%	4.7	3.2%
Non-Classifiable Establishments	2%	1.7	3.4%
Mining	1%	3.0	10.3%
Construction	<1%	1.7	1.1%
Agriculture, Forestry, & Fishing	<1%	1.4	2.0%
Non SIC Related Industries			
Energy	2%	2.0	8.4%
Healthcare	<1%	2.0	1.1%

Source: Symantec 2016 Internet Security and Threat Report

# Email Phishing Tactics

If cyber crime were an industry, it would rank among the most innovative. Every day, thousands small business owners (i.e. criminals) find new ways to improve their products and marketing (i.e. their malware and phishing).

Phishing emails use many tactics but their goal is always the same: to steal information from the user (usually login credentials credentials).

Attackers use phishing to steal the information in one of two ways:

1. Install malware on the user's system and secretly steal data. One example is a Trojan that captures the user's login credentials and sends them to the attacker.
2. Trick the user into sending the information directly. One example is by asking the user to enter login credentials on a spoofed webpage controlled by the attacker.

The most common way (by far) is to install malware on the victim's system.

"The majority of phishing cases in our data feature phishing as a means to install persistent malware," according to the Verizon 2016 DBIR.

This section describes common tactics that attackers use in different components of an email phishing campaign. The number tactics is so fluid and dynamic that it's easy to be overwhelmed (and impossible to list them all). To stay grounded, remember that the goal of phishing is to steal the user's information and that it is typically done in one of the two ways listed above.



# Email Phishing Tactics

## 1. From Name and From Address

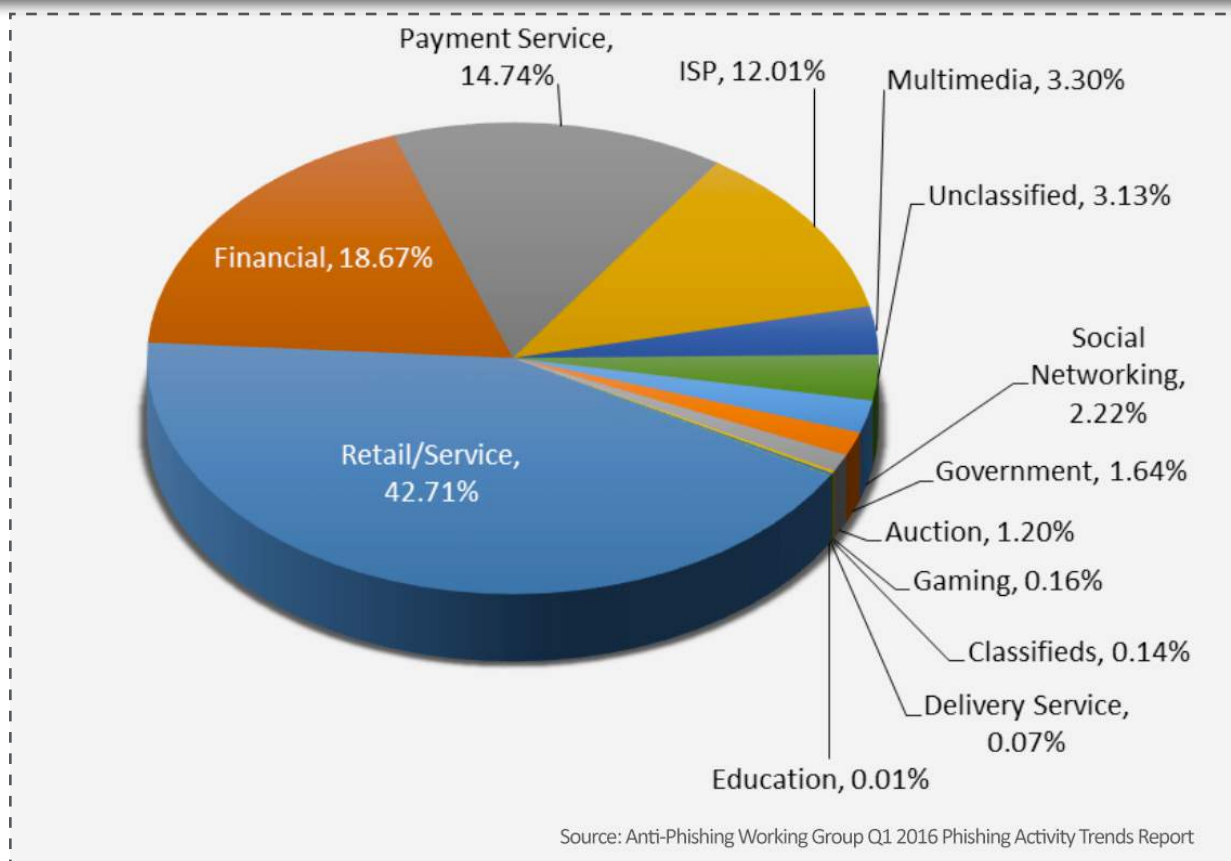
Phishing emails want to earn trust. One approach is by impersonating – or spoofing – well-known brands.

The most commonly spoofed brands are in the retail and service sector, according to the chart below from the Anti-Phishing Working Group Q1 2016 Phishing Activity Trends Report (PATR).

Brands in the retail, financial, and payment service sectors make up more than 75% of the brands spoofed in the emails reviewed in APWG's report.

**Note:** the PATR use “targeted industry sector” to describe the brands that are impersonated by attackers in campaigns. Our report defines “targets” as the recipients of phishing emails.

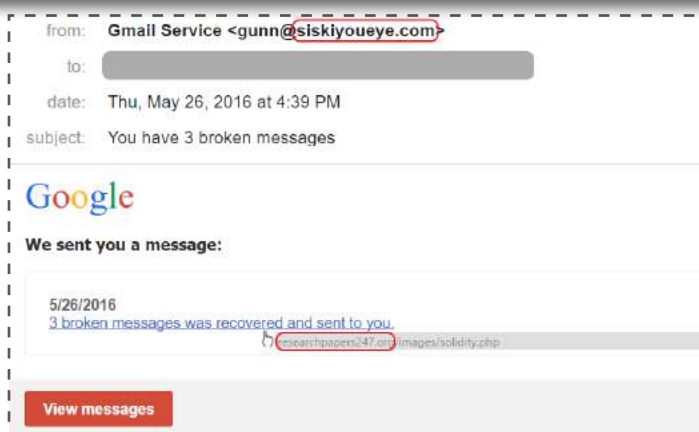
### Most Targeted Industry Sectors 1<sup>st</sup> Quarter - 2015



# Email Phishing Tactics

## 1. From Name and From Address

### Fake Gmail Email Spoofing Example



Some phishing messages do a poor job of spoofing the sender's address. In the example above, the email's From Name is "Gmail Service" but the From Address is unrelated to Google or Gmail.

Why would Gmail send a message from an unrecognizable domain? This is a clear red flag.

In other cases, the attacker may change the first portion of the From Address (i.e. the username or local part) to mimic the brand. For example, the address "gmail@siskiyoueye.com" appears more legitimate at a glance than the example above. Attackers can easily alter this portion of the address.

The attacker can also work harder to disguise the second portion of the From Address (i.e. the domain or portion after the "@"). One way is with a homograph attack, which uses visually similar characters to spoof URLs.

For example, the address support@amazon.com can be faked by replacing the "o" in Amazon with the Greek letter "ο" which is identical but technically a different character and therefore in reference to a different domain.

Targeted phishing attacks may attempt to earn trust without using brands. One way is to impersonate a fellow employee at the target's company. By including the employee's name in the From Name, or by spoofing the employee's email address, an attacker can make the message appear to come from a trusted source. Another approach is to use the recipient's business or personal name in the email's From Name or subject line to make it appear more relevant.

# Email Phishing Tactics

## 2. Subject line

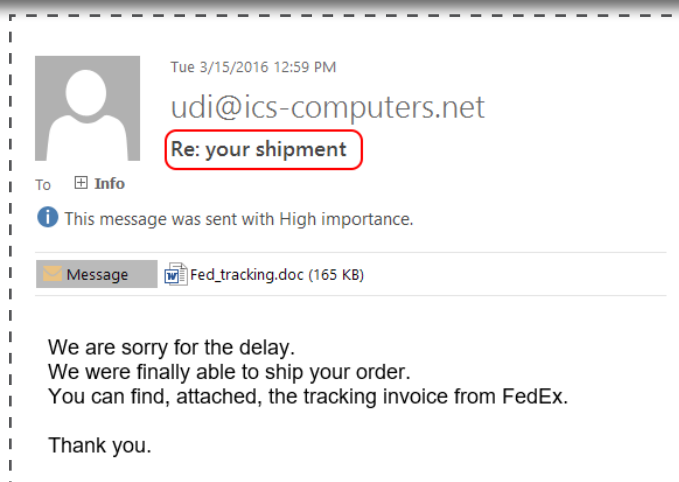
Phishing attackers have a tiny amount of space in which to convince people to open their emails. They have the From Name and Sender Address. They also have the time the email is sent. Aside from that, the only other part of a message that can significantly influence its open rate is the Subject Line.

Phishing emails will use old tactics in Subject Lines, such as beginning with “RE:” to try to fool the recipient into believing the email was sent as a response. Some have added personalization by dynamically including the recipient’s name or company name.

In the business world, a typical approach is to disguise the email as an important, time-sensitive message, such as an invoice or customer complaint. Simple subject lines such as “Invoice: 78952” or “Shipping notice” are common.

As you will see, phishing Subject Lines take a similar approach to the Body of the emails. They want to trick the recipient into believing the message is an urgent and relevant matter that should be dealt with immediately.

### Time-Sensitive Email Example



# Email Phishing Tactics

## *3. Body of the message*

In a phishing email, the timing, sender, and Subject Line are designed to pique the recipient's interest. Once he is reading the Body, he is nibbling at the bait. He is one nibble away from getting caught. The Body is designed to make him take that bite.

Phishing emails that impersonate well-known brands are likely to include the brand's logo. This is to build trust. Major brands spend millions of to give consumers a sense of assurance when they hear the brand's name or see its logo. The attacker is trying to hijack this trust.

In business, phishing emails that do not use brand names tend to claim to have been in recent contact with the person. They ask the recipient to reply, click a link, or download an important attachment.

# Email Phishing Tactics

## 3. Body of the message

### Phishing at Calyptix

To the right is an example of a phishing email received by a Calyptix employee that claimed to be from an upset customer. The email is very simple, but includes a few elements that make it more convincing:

1. The email refers to an order that was placed. This fits because Calyptix is a business.
2. Our domain, Calyptix.com, is mentioned (although it is incorrectly used as our company name)
3. The email is signed with a person's name, company name, phone, and fax number.

People do not think clearly under stress, which is why some phishing emails try to pressure the recipient. They may threaten to close the person's account or impose a fine if action is not taken. They may offer a large cash prize to get the person excited. In the example to the right, the attacker hoped that a customer complaint would spark the recipient to act without thinking.

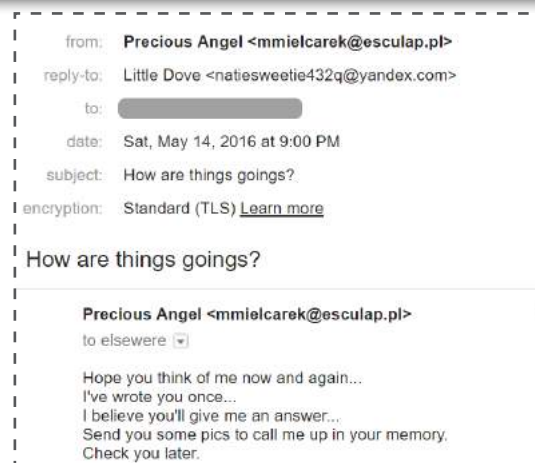
In personal settings, phishing emails often promise prizes or "opportunities." They may masquerade as advertisements for popular brands, and they may also appear to come from sexually suggestive strangers, as shown on the lower-right.

Some phishing messages ask the person to call a phone line. On the call the victim is usually directed to share credentials or other personal information, or install malware or a remote desktop tool.

### Calyptix Phishing Email Example



### Personal Phishing Email Example



# Email Phishing Tactics

## 3. Body of the message

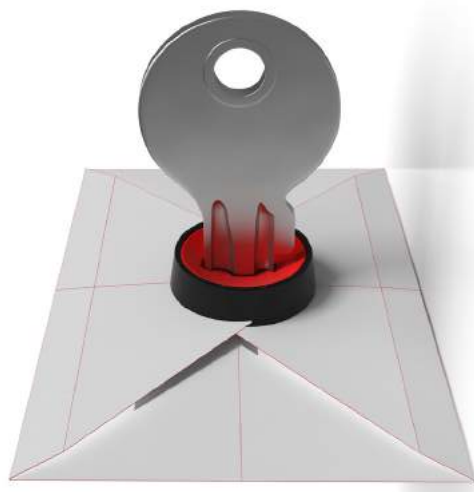
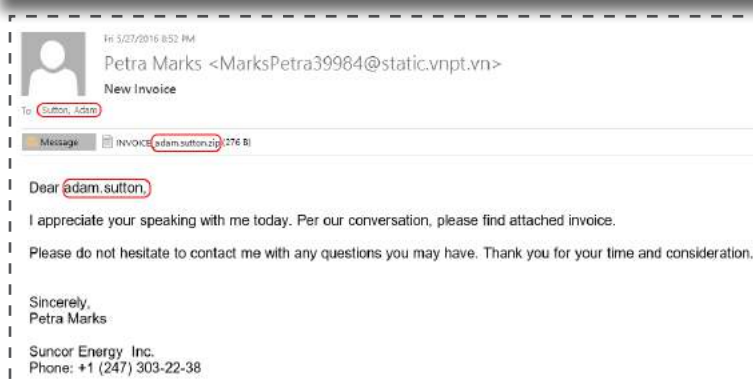
### Phishing is more personal

More attackers are personalizing their phishing attacks. Their emails may include tidbits of personal or professional information, such as details from the target's public profiles on Facebook or LinkedIn. It may reference other employees at the company who the attacker discovered on LinkedIn or another public website. The message can also reference recent company news and other details if the attackers take time to read through the firm's press releases and press mentions.

Personalization does not always have to be complex. Sometimes simply including the recipient's address, domain, or company name is enough to make the message more convincing. In the example to the right, you can see the recipient's email user name is used both in the Body of the email and in file name of the attachment.

All of this personal and professional information is designed to make the message more believable to make it easier for the recipient to take the attacker's desired action: to click a link, download an attachment, or respond to the message.

### Personal Phishing Email Example with User's Information



# Email Phishing Tactics

## 4. Malicious links

Many times the action a phishing email urges the recipient to take is to click a link. The website that awaits can have nasty surprises, but first the victim must click.

Below are some of the tactics used to disguise link URLs and trick people into clicking links.

**Subdomains** – An email that appears to come from Wells Fargo may ask the user to click a link to <https://wellsfargo.reallysafebanking.com>. However, this site has nothing to do with Wells Fargo's real website, [www.wellsfargo.com](http://www.wellsfargo.com). Instead, the primary domain is [reallysafebanking.com](http://reallysafebanking.com), and the "wellsfargo" portion of the URL is only a subdomain intended to trick the user into a sense of safety.

**Similar characters** – As mentioned above, attackers can use deceptive characters to fake a domain address. This also applies to the domains of destination URLs in hyperlinks. For example, an upper-case "I" can be used in place of a lower case "l" to make a spoofed domain such as [www.wellsfargo.com](http://www.wellsfargo.com) or [www.paypal.com](http://www.paypal.com) seem legitimate.

In lowercase, these addresses are as follows: [www.weiisfargo.com](http://www.weiisfargo.com); [www.paypai.com](http://www.paypai.com). The Greek alphabet also has characters that look nearly identical to E, n, k, v, o, p, t, u, and x.

**Short link aliases** – Link-shortening services, such as bit.ly, can take long URLs with 100 or more characters and return a new, shorter URL to the same page, such as <http://bit.ly/1TTgSY6>. Using these shortened URLs as link destinations is another way attackers can obscure the true address.

**Misspellings** – It's easy to overlook the reversal or omission of a couple characters in a URL, which is why misspelled versions of a spoofed brand's domain are common in phishing links. Examples include [www.bankofammerica.com](http://www.bankofammerica.com) and [www.americanexpres.com](http://www.americanexpres.com).

**Misleading link text** – A hyperlink may say <http://www.ebay.com> or visit eBay's website but clicking it may lead to a different destination than indicated in the visible text.

**IP addresses** – IP addresses are the true destination when browsing the web. Attackers can use the IP address of a malicious site as a link's destination URL to hide the destination from users.

# Email Phishing Tactics

## 5. Malicious attachments

Most phishing attacks aim to install persistent malware on a victim's machine, according to data from the 2016 DBIR. One of the most common ways is to convince the user to open a malicious attachment.

The message may claim that the attachment is an invoice, payment information, or simply "details" as shown in the earlier examples.

Documents from the Microsoft Office suite of products – such as Microsoft Word and Excel – are the most common file types seen in malicious attachments. No surprises here – they are also among the most popular types of legitimate file attachments.

Microsoft Word (.doc) files make up more than half of the malicious attachments seen in 2015, according to the chart to the right from the Symantec 2016 ISTR.

### Malicious File Attachments in Email

Rank	File Extension	Blocked in Emails
1	.doc	55.8%
2	.xls	15.0%
3	.zip	8.7%
4	.htm	7.9%
5	.docm	2.4%
6	.js	2.2%
7	.mso	1.9%
8	.html	1.6%
9	.exe	0.9%
10	.png	0.8%

Source: Symantec 2016 Internet Security and Threat Report

# Email Phishing Tactics

## 6. Malicious Websites

Clicking a link in a phishing email may begin a download of malicious software, but it can also lead to one of two kinds of websites.

### Phishing websites

The first is a phishing website. These sites appear to be from legitimate brands and usually ask the user to enter some information, such as login credentials.

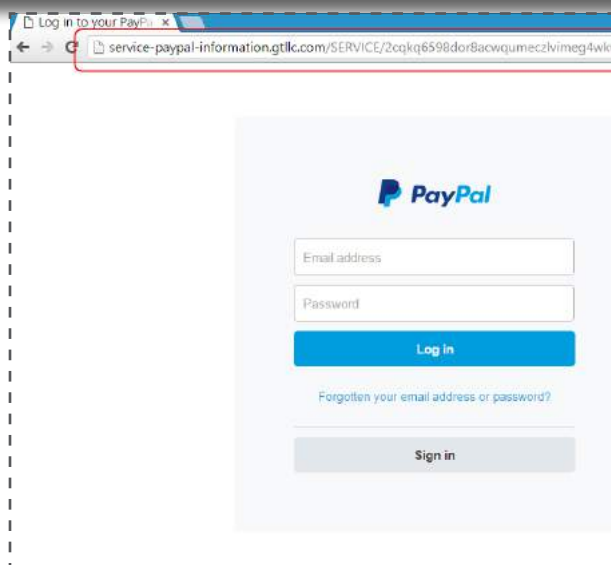
One obvious sign of a phishing website is that it requests important information but does not show a green lock icon in the address bar. The green lock icon indicates that the user's connection to the site is encrypted. Banking websites, ecommerce websites, and any others that request personal information should always display this green "secure" icon.

However, many phishing websites lack this indicator, which is a sign that something is wrong. The example below compares a spoofed PayPal login page to a legitimate one.

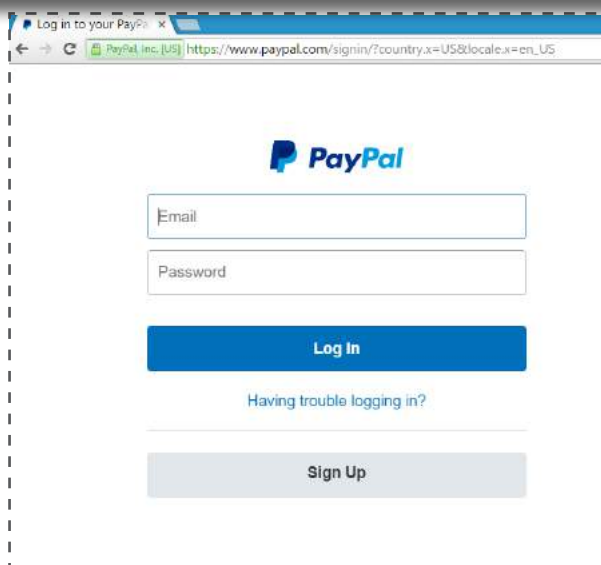
The site may use visual deceptions, such as images or overlays to hide the browser's address bar. They may also imitate the green padlock of legitimate websites that use encrypted HTTPS.

Sometimes the website is legitimate and has been compromised by the attackers. In these cases, the user will click to visit a legitimate site. The legitimate site loads but with an overlay form from the attackers that requests login credentials. Compromised sites can also redirect visitors to a malicious site controlled by attackers.

### Paypal Example - Fake



### Paypal Example - Legitimate



# Email Phishing Tactics

## 6. Malicious websites

### Malware websites

Oftentimes the website has no intention of collecting personal information. Instead, it attempts to force malware on to the user's system. This usually happens by exploiting an unpatched vulnerability in the user's browser or another application, such as Java or Flash.

Once the malware is on the user's machine it acts as a Trojan, monitoring the victim's behavior and keystrokes to collect sensitive information – such as banking and system credentials – to export to the attacker.

These sites can also encourage users to download and install the malware themselves by disguising it as legitimate software.



# Email Phishing Tactics

## 7. Filter evasion

Email phishing is a game of cat and mouse. The mice constantly find new ways to bypass spam filtering, and the cats constantly chase them out of the inbox.

The number of tactics that attackers use to evade detection is too great to fit into a simple report. Three basic approaches are listed below to give you an idea.

- Use of images instead of text to avoid being flagged as spam based on the content
- Continually rotating email domains and recirculating IP addresses to evade blacklisting
- Using white text on white backgrounds as filler to make the email's overall content seem more legitimate



# How to Avoid the Hook

Cyber attacks are like the flu. You can avoid it – by washing your hands, staying warm, etc. – but you cannot eliminate it.

Technology can help. Training users can help. But nothing can “fix” it. If a business accepts inbound email (and who doesn’t?), then it is almost certain to receive phishing emails, and some of them will reach end-users.

A multi-layered approach is best, one based in technology, training, and preparing for the worst-case scenario.



# Steps for MSP & VARS

## 1. Train users to recognize phishing attempts

Most of your clients do not have the skills to deploy anti-spam and anti-phishing technology. They rely on you to take steps, such as the suggestions below, to help keep them safe.

Users are the biggest challenge and the best solution to email phishing. Without proper training, it's only a matter of time before one clicks the wrong link or opens the wrong attachment.

However, with the right guidance, even the most tech-challenged clients can learn to avoid obvious phishing emails. Below are a few ways you can help.

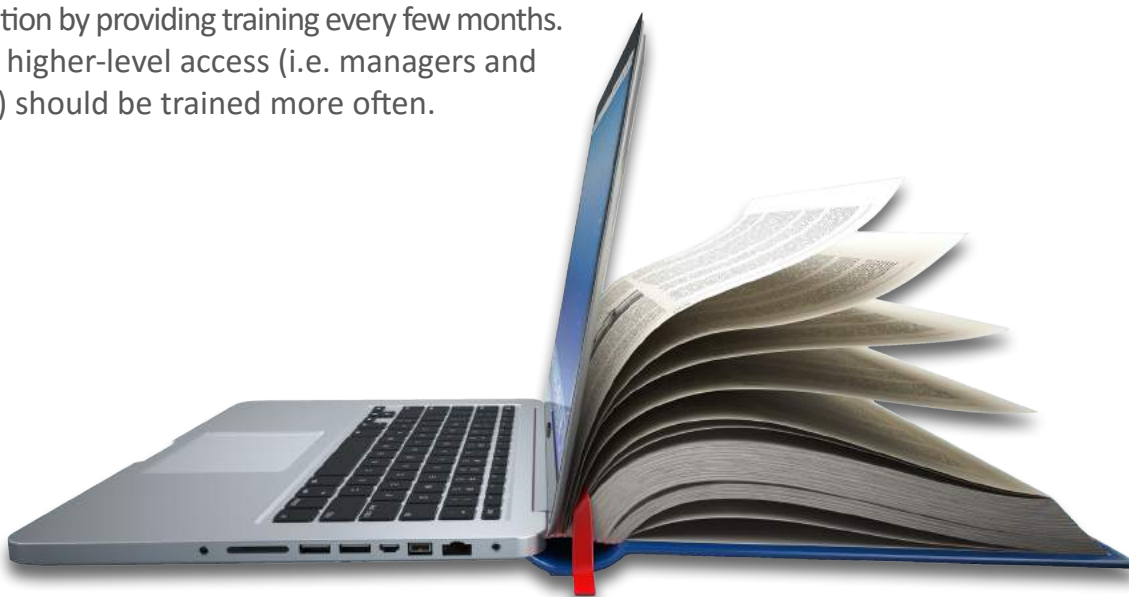
**Provide a hand out** – Explain how phishing scams work and what phishing emails look like. Clients should be able to keep the handout at their desks.

**Train regularly** – Rather than a one-off effort, reiterate the information by providing training every few months. Users with higher-level access (i.e. managers and executives) should be trained more often.

**Simulate attacks** – Create and send phishing emails to your clients unannounced. Link the email to a webpage that tells users that they have been phished and gives tips for improvement. Several paid solutions, such as Wombat and PhishMe, are available to make this process easier.

**Show examples** – Demonstrate the qualities of good email against the qualities of suspicious email. The examples will make your lessons more concrete.

**Explain the risks** – A simple phishing attack can lead to a major data breach for the organization. A breach can invite costs tied to forensic analysis, regulatory fines, litigation, and alerting customers. Smaller organizations can be forced to close after an attack. Show examples of companies that have been victims of these attacks to make the message sink in.



# Steps for MSP & VARS

## *2. Create a reporting system*

Allow users to forward suspicious emails, or otherwise mark them, so they can be reviewed. Serious attacks can then be shown as examples to put the rest of the company on alert. Some organizations, such as Cornell University, post a list of recent phishing emails received.

Also consider incorporating a reporting process to third parties, such as the US CERT (see the resources at the end of this report for links to Cornell's list and the US CERT).



## *3. Secure file sync and share*



Email attachments are a popular way for attackers to breach a user's system, but they are also a business reality. Eliminating them is not an option for most clients.

However, if they are open to the idea, solutions exist that make it easy for clients to share files without the use of attachments. Instead, the file is loaded onto a secure server and a link to download is pasted into the email.

Organizations that are willing to adopt a sync-and-share system can eliminate the use of attachments and thereby disregard a large portion of inbound phishing emails. Unfortunately, this requires a major change in a well-entrenched user behavior.

# Steps for MSP & VARS

## 4. Anti-virus



Signature-based anti-virus can help prevent malware infections, but it has become less effective in recent years. Attackers are learning to craft malware that automatically alters itself to establish a new hash-signature, thereby making it unknown to conventional anti-virus products.

However, not all malware variants are altering themselves in this way, and anti-virus can still prevent many infections. It remains a good tool, but is less reliable.

## 5. Patch, Patch, Patch

One of the most important steps is to keep your clients' systems up to date. Firmware, operating systems, anti-virus, browsers, and other applications such as Java, should all be updated as soon as a new patches are available. Apply patches automatically when possible.

Patching will ensure that any known vulnerabilities will be repaired. This makes it more difficult for attackers to penetrate a system and install malware.

Patching will not prevent all attacks. Zero-day attacks, which exploit vulnerabilities that are unknown to vendors, are a threat. However, most exploits are for known vulnerabilities for which vendors have issued a patch, and many have been known for a year or longer. This is why patching can prevent many common infections.

# Steps for MSP & VARS

## 6. Spam filtering

Email servers should use a high-quality spam filter to stop phishing emails from reaching end users. Effective filters will weigh multiple factors – such as a message’s content, authentication, source IP, attachments, and others – and apply a score to each inbound email.

Messages should also be scanned against spam blacklists, virus signatures, and other resources to detect known threats.

Emails that score above a given threshold will be flagged as spam and sent to a spam folder or quarantine. The administrator should be able to adjust the spam-score threshold to calibrate the filter and control the quality of emails that are allowed to pass.

**Email quarantines** – The email spam folder or quarantine should be a safe environment in which suspicious emails can be inspected. The system should display the email’s country of origin, detailed header info, and content without the risk of infecting the user. Emails that are marked as safe should pass through the filter and arrive at the user’s inbox. Each user should have a quarantine that he or she is trained to maintain.

**Filter by geography** – Many businesses operate only within the U.S. or North America. If this is the case for your client, then consider filtering their email traffic to block all inbound messages from overseas. This will eliminate emails that come from servers overseas. Although most malicious email is sent from within the U.S. a good portion is sent from outside the country.

**Blacklists and whitelists** – Blacklisting is also a good option. Look for solutions that use a combination of blacklists – such as those maintained by third parties that specialize in listing spammers and threats, and one maintained by your organization that lists source IPs that are deemed malicious.

Whitelists can also be an effective tool to ensure safe delivery of trusted senders. An extreme option is to use whitelist-only, which allows only messages from a given list of senders to be delivered.

Whitelist-only can be difficult to implement for organizations that accept inbound requests from unknown senders, such as potential customers. However, if it can be used, it’s an effective way to significantly cut the risk of phishing emails.



# Steps for MSP & VARS

## 7. Think beyond email

A user will be tricked by a phishing email. It's inevitable. Rather than hope the day never comes, a better approach is to prepare for it.

**Segment networks** – Do not host every business asset on the same LAN. Instead, separate high-risk systems – such as user terminals and guest wireless networks – from business-critical assets, such as point-of-sale systems and customer databases.

**Filter websites** – Deploy a web filter that monitors and controls the websites that users can access. This will block many malicious websites and blacklisted URLs. Also consider a whitelist-only policy, which allows users to access only websites that are approved by the administrator. That way if a user clicks on a link in a phishing email then the website is unlikely to load.

**Strong authentication** – All critical systems, such as customer databases and personal info, should require strong passwords. Consider a two-factor authentication system, such as one that requires the user to enter a password and then enter a passcode sent via text message.

**Standard user accounts** – Do not allow users to browse the web or check email while logged into Administrator accounts on their machines. Unless it is absolutely necessary, users should operate as a Standard user. An Administrator password should be required to install software, uninstall software, or change system settings.

**Back up files** – Maintain fresh backups of important systems and files. Make sure they are disconnected from the network, since network shares can be compromised during a successful attack or malware infection.



# Advice for your Clients

You are your client's trusted advisor on technology and security. They need your advice to keep their business networks safe and running.

Be sure to emphasize that all the technology in the world cannot stop phishing emails. It takes only one user to click one email for a problem to erupt. The best way to stay safe is to educate users until they are intelligent and vigilant in the inbox.

Share the tips on the following pages with your clients to make them better judges of email.



# Advice for your Clients

## 1. Stop and think

Email is one of the most common ways for a cyber attack to begin. Do not open your emails on auto-pilot. Stay aware.

Three actions that can get you in trouble with a phishing email:

**Clicking on it** – Clicking on links or images in a phishing email will take you to a website that will either try to force malware onto your computer or it will try to trick you into sharing important information (like passwords). Always be careful before you click.

**Downloading the attachment** – Attackers often send malware as an email attachment. It might look like a harmless file, such as one from Microsoft Word or Excel, but they are dangerous. Do not click these files. If you accidentally download one, delete it immediately.

**Responding** – Some phishing emails will ask you to respond by calling a phone number or by replying to the email. Do not respond to suspicious emails. If you want to reach the alleged sender, then manually type the company's web address into a browser. Do not click a link in the email.

If your suspicions are raised even slightly, do not open or click the email. Forward it to your IT expert or a phishing alerting system.



# Advice for your Clients

## *2. Inspect links before clicking*

In emails, hover your mouse over links before clicking them. This will show the destination URL. Does the address make sense for the link?

For example, if the email is from UPS, does the link show a UPS address? Or is it for another website? If the destination URL does not match your expectations, then do not click the link.



## *3. Never send private information via email*



Legitimate companies will never ask you to send passwords, credit card numbers, social security numbers, or any other important information via email. Any emails that request this information should be considered highly suspicious.

# Advice for your Clients

## 4. Judge the email's content

Be very suspicious of any email that includes the following:

**Poor spelling** – Some attackers are from overseas and their grasp of the English language is not perfect. Look for misspelled words and incorrect grammar.

**Threats** – People who are under pressure do not make good decisions. Attackers know this and will threaten to close your account, charge you a fine, or take something from you. These are threats, and any email that threatens you is suspicious.

**Urgency** – Similar to threats, this tactic is designed to make you feel pressured into acting before you have a chance to think. Messages that demand an immediate response are suspicious. For any email that demands an immediate action, take a deep breath and ask yourself – is this a scam?

**Unsolicited** – A seemingly random email from a business with which you have no recent dealings is suspicious. For example, if you receive an invoice for an order, even one from a familiar vendor, be very suspicious if you cannot remember the reason it was sent.

**Attachments** – Never open attachments from senders you do not recognize. Also do not open attachments that you were not expecting, even if they arrive from addresses you recognize.

**Common themes** – Attackers have thousands of tricks. A common approach is to ask you to reset, update, or confirm account information. Never click an email that asks you to supply account details. If you think it might be legitimate, then contact the sender directly via telephone or by typing the company's URL directly into your browser.

Also consider using plain-text to view all of your emails. This makes it harder for the attackers to hide content and will reveal the true destination URL for all links in the message.

**Remember:** clicking is the number-one way to get into trouble. If you are unsure or suspicious, then never click on the email or attachment.



# Advice for your Clients

## 5. Judge the webpage

Some phishing emails will lead to a spoofed webpage, i.e. one that has been made to look legitimate but is actually controlled by the attacker. These pages typically try to get you to enter information – such as passwords or banking info. They may also try to infect you with malware.

Here are some ways to spot phishing webpages. If you land on one, close your browser immediately and alert the IT administrator.

**Pop ups** – Never enter information into a pop-up screen, even one from a legitimate website. Some attackers will penetrate honest websites and inject a popup form to steal information from visitors.

**Overlays** – On some webpages, the attackers will block the web address by putting an image over the address bar. If something does not look right about the address bar, or if you see an image load over it, do not proceed.

**Poor spelling** – As mentioned above, some attackers are not fluent in English and will make spelling mistakes in a page's content. Although less common than in the past, this remains a dead-giveaway.

**Check the certificate** – Websites that ask you for important information – such as banking credentials and personal info – should be secure (i.e. encrypted). Check the browser bar for the green pad lock icon, and check that the web address starts with “https” instead of “http”.

If you are suspicious, also click on the green padlock icon in the browser bar. One or two more clicks will reveal the site's encryption certificate which you can confirm is real.

In all cases – whether for an email, website, or link – use your instincts. If something does not feel right, then do not click or respond. It's better to be safe than sorry.



# Advice for your Clients

## 6. Judge the URL

This applies to both email addresses and webpage addresses. Attackers will try to fake legitimate web addresses by disguising their own.

If you see any of the following, be very suspicious:

**Similar characters** – Some addresses will look almost like the real address, but not quite. For example, [www.google.com](http://www.google.com) might be faked as [www.goog1e.com](http://www.goog1e.com).

**Subdomains** – When you look at an address, always read it from left to right. The last domain in the address is the true domain. Anything that comes before it is irrelevant.

For example, [www.paypal.totallysafesite.net](http://www.paypal.totallysafesite.net) and [www.paypal.jkiuoiondfa.889zxx0.totallysafesite.net](http://www.paypal.jkiuoiondfa.889zxx0.totallysafesite.net) have nothing to do with PayPal. Instead, they are from [totallysafesite.com](http://totallysafesite.com). The site just created a subdomain called “paypal”, which any site owner can create.

# Sources

**Alan Paller, Director of Research, SANS Institute: Quote**

<https://blogs.mcafee.com/business/put-phishing-knowledge-test/>

**Symantec 2016 Internet Security Threat Report**

<https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

**Verizon 2016 Data Breach Investigations Report**

<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

**McAfee Phishing Deceives the Masses: Lessons Learned from a Global Assessment**

<http://www.mcafee.com/us/resources/reports/rp-phishing-quiz-assessment.pdf?snsdpd-0115>

**Anti-Phishing Working Group: Q1 2016 Phishing Activity Trends Report**

[https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2016.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf)

**U.S. Computer Emergency Readiness Team (CERT): Report Email Phishing**

<https://www.us-cert.gov/report-phishing>

**Federal Trade Commission (FTC): Report Email Phishing**

<https://www.consumer.ftc.gov/articles/0003-phishing>

**PhishMe: Security Behavior Management**

<http://phishme.com/>

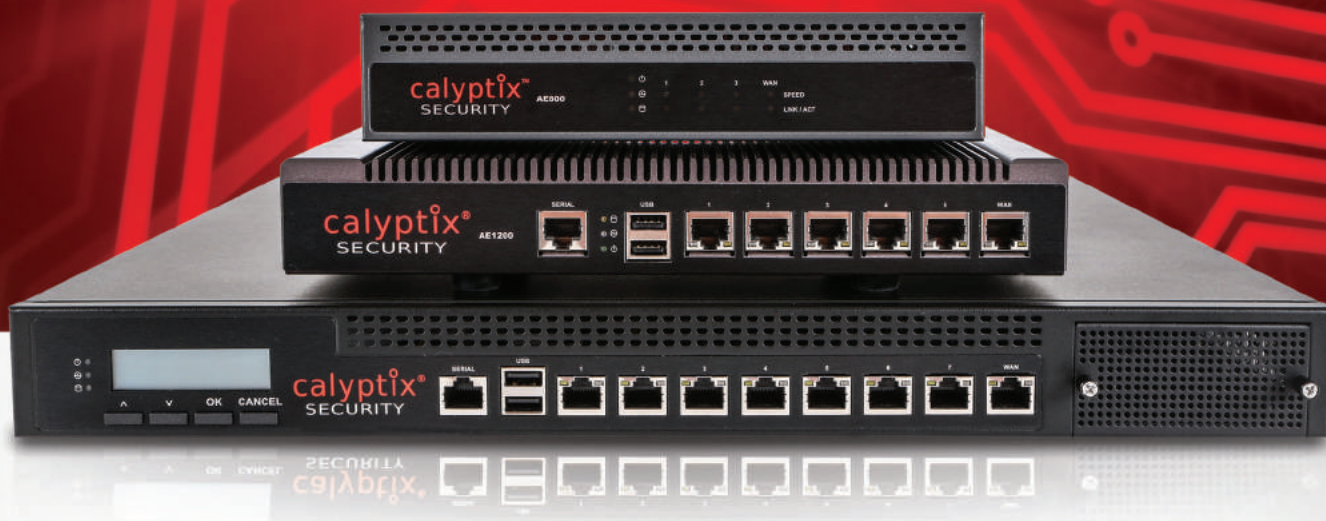
**Wombat: Security Awareness and Training Software**

<https://www.wombatsecurity.com/>

**Cornell University: Phish Bowl – Phishing Email Examples**

<http://www.it.cornell.edu/security/phishbowl.cfm>

# Tough on hackers. Easy on your budget.



## AccessEnforcer

Network security is easy with the AccessEnforcer UTM Firewall from Calyptix. First, you save time and protect clients with an easy-to-use firewall. Second, you solve problems faster with unbeatable tech support. Third, you increase profits with a reseller program that fits your business model.



Secure your network  
completely



Make security  
simple



Improve uptime  
& reliability

See what easy security looks like with Calyptix  
[www.calyptix.com/partners](http://www.calyptix.com/partners)

**calyptix**<sup>®</sup>  
SECURITY