2019

Email Security Best Practices

How to keep your organization from getting phished

Enterprise insights on how to better secure email servers, train staff and defend your organization against phishing.

By Patrick Nohe & Ross Thomas

The SSL Store™

146 Second St. N., Suite 201

St. Petersburg, FL 33701

(727) 388-4240

sslstore

hashedout by The SSL Store™

91% of cyber-attacks start with a Phishing Email

The Nigerian prince has grown up, nowadays 97% of people can't spot phishing emails.

In March of 2016 the toy company Mattel was undergoing a transition period. You know Mattel—it makes the Barbie dolls, Hot Wheels and WWE action figures that used to line the shelves of the now-shuttered Toys'R'Us (RIP Geoffrey). The new CEO was Christopher Sinclair. His predecessor had been fired. And the entire company was navigating through a period of corporate change.

That's why it didn't raise any eyebrows when the new CEO emailed an executive requesting a new vendor payment. Mattel company protocol requires two executives to sign off on any fund transfers. With the CEO, Sinclair, having already signed off on it, the unnamed executive rubberstamped the transfer and Mattel wired $3,000,000 to a bank in Wenzhou, China.

A few hours later the executive mentioned the transfer to Sinclair, who had absolutely no idea what she was talking about. Mattel had been phished by enterprising criminals who took advantage of the company's recent turnover and imitated its new CEO.

This was easily preventable with S/MIME certificates and email signing. Had Mattel deployed email certificates at scale, the executive would have been tipped off by the lack of a digital signature. Instead, because of the recent upheaval, the phishing attempt worked perfectly.

This kind of CEO fraud (and other types of phishing incidents) can and will get people fired, too. There are more than a few cases of employees being fired for falling for phishing emails. Sometimes culpability goes all the way up to the C-suite. In 2016, Austria's Fischer Advanced Composite Components AG (FACC) fired its CFO and its CEO after it got phished. And just last year, a Dutch court determined that cinema company Pathé had cause to fire its CFO and managing director for failing to spot a phish. If your company gets phished, heads WILL roll. And the only thing that can quench the angry flames smoldering in the board room post-phishing is the blood of a young IT admin.

Mattel represents a great cautionary tale for businesses of all sizes. And there are three big lessons that we can take from it.

1. Phishing can happen to anyone, anywhere

It's nice to think that these kinds of phishing scams only happen to large, enterprise companies but that couldn't be further from the truth. Small businesses are hit with nearly the same frequency as their larger counterparts. In fact, three out of four SMBs report they've been the target of at least one phishing scheme in the past year. Take for example the incident that cost Edmonton's MacEwan university $11.8 million. There's no way that a bunch of Edmonton construction companies thought they would become the victims of a phishing scheme targeting a Canadian university. Likewise, I'm sure the administrators at MacEwan felt the same way.

76%

Of SMBs dealt with phishing last year

2. These phishing schemes are sophisticated

In the early days of the internet, the most infamous examples of phishing were those random, poorly spelled pleas from someone professing to be Nigerian royalty. The typical MO was that this Nigerian prince was having some kind of problem getting a bunch of money out of the country and he promises to reward you with some of it if you send him some money to help him get everything figured out first. We're light years beyond that now. Today's most effective phishing scams are meticulously crafted, using highly convincing imitations of known brands or scraping information from social media sites like LinkedIn to socially engineer believable situations. They're tossing SSL certificates on their phishing sites to make them look more legitimate. And 97% of internet users can't spot a convincing fake.

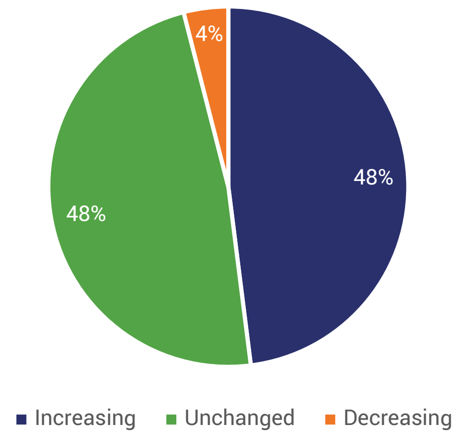
3. S/MIME Certificates could have prevented this

Like so many other organizations, Mattel had very little in place to help prevent this situation. While there was a policy that required to executives to sign off on any transfers, the recipient didn't bother to verify that the email was authentic, which is much harder without S/MIME certificates and email signing. If Mattel had a policy in place requiring email to be signed and employees to check for the signature this never would have happened. Not only did Mattel almost lose $3-million (it was able to recover the money thanks in part to a Chinese banking holiday), this event was widely covered in the media (and by at least one eBook) and did damage to the toymaker's reputation.

Mattel isn't alone in being unprepared. Most organizations are. And their employees are even more unprepared. According to a McAfee survey, 97% of consumers couldn't ferret out a phishing attempt (a phishing email is oftentimes called a "phish"). In fact, that's just one of many terrifying statistics that underscores just how pervasive a threat phishing is. Here are a few more:

- 70% of US employees have no concept of cybersecurity best practices (Source: Hashed Out)
- 1 in every 101 emails sent in 2018 was malicious (Source: FireEye)
- 76% of organizations reported receiving phishing attempts in 2017 (Source: Wombat Security)
- 53% of organizations reported receiving spear-phishing attempts in 2017 (Source: WS)
- 49% of phishing websites are now using HTTPS (Source: Hashed Out)
- 49% of successful phishing attempts result in malware infections (Source: WS)
- 38% of successful phishing attempts result in compromised accounts (Source: WS)
- Phishing resulted in over $12-billion in direct losses in 2017 (Source: FE)
- Phishing attempts grew by 65% in 2017 (Source: FE)

Organizations say the rate of phishing attacks is…



Phishing is actually kind of a catch-all term, but there are myriad varieties – some of them don't even involve email – and then there are email attacks that technically don't constitute phishing but get lumped in anyway. For the sake of this eBook, we'll limit our discussion to email-based attacks.

Phishing: A crime with two victims

Phishing is a unique cybercrime in that it really has two victims: the company being imitated and the company being targeted. Unfortunately, a lot of the phishing statistics you see conflate these two things, which means it can be difficult to get reliable data. But regardless of whether you're the one being spoofed or the one being duped – chances are you're going to end up dealing with phishing at some point in 2019. One of the biggest takeaways from the MacEwan incident was that any company or organization can be victimized by phishing. According to Wombat Security, 76% of organizations have experienced a phishing attempt in the past year. And that shows no signs of abating.

Let's start by talking about the companies and industries that get imitated. Knowing who the most commonly spoofed brands are can help inform the mitigative strategies we'll be discussing in the second half of this paper. Phishing attacks that imitated a Software-as-a-Service increased 237% in 2017, and as the SaaS model becomes more proliferated these attacks look to continue to increase in frequency and severity.

On the other hand, the financial industry has actually seen a steady decline in its share of phishing attacks. While the number of attacks has remained fairly static, its share has fallen from 38% in 2013 to just 20% in 2017. Granted, that still means one out of every five phishing attacks is impersonating the financial industry.

Industries Most Imitated in Phishing Attacks

Email/Online Services	Financial	Payment Services	Cloud Storage/File Hosting	E-Commerce
26.1%	20.5%	16.1%	13.8%	7.6%
+26%	-11%	+14%	-40%	-32%

Software-as-a-Service	Social Media Networks	Dating Sites	Government Services	Other
7.1%	4.5%	.9%	.5%	3%
+237%	+190%	-44%	-70%	--

Companies Most Imitated in Phishing Attacks

Microsoft	PayPal	NETFLIX	Bank of America	WELLS FARGO
1st	2nd	3rd	4th	5th
+23.7%	+29.9%	+61.9%	+57.4%	21.5%

Facebook	CHASE	orange™	DHL	Dropbox
6th	7th	8th	9th	10th
-35.6%	+352.2%	+92.8%	+2.6%	+.3%

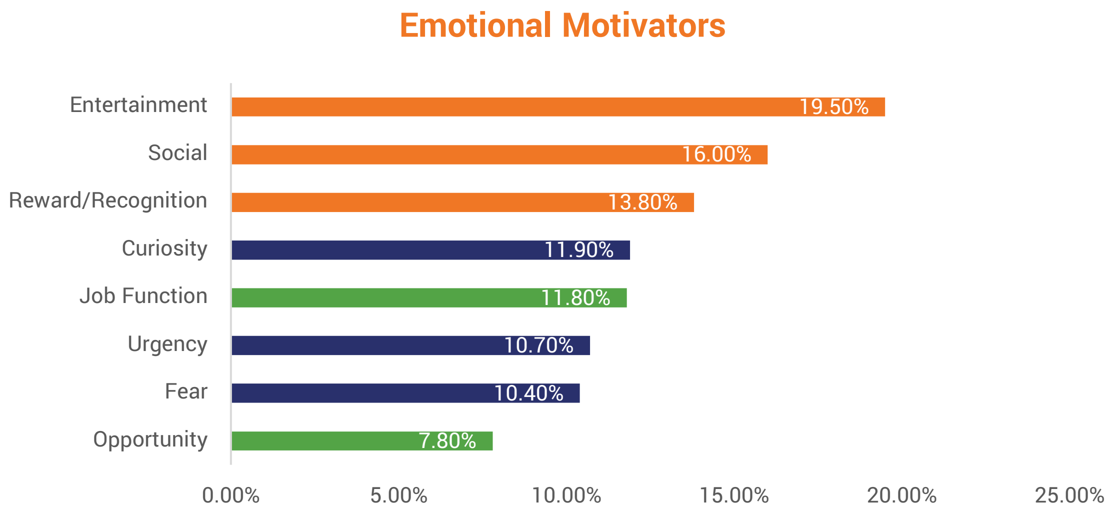
Phishing your emotions

The best phishing emails have historically been designed to create a sense of urgency, fear or curiosity in the recipient. The industries and companies that are most often imitated tend to lend themselves towards that end. While there are myriad ways to build a phishing scam, there are some techniques that are much more prevalent than others:

- CEO Fraud – The attacker imitates the company's own CEO or another high-level executive and emails lower level employees directly hoping to elicit the intended reaction.
- Whaling – A type of Spearphishing attack targeted at high-level company executives, like VPs and the C-Suite.
- Spearphishing – The attacker does research on the target, often consulting social media profiles and other publicly available information in order to socially engineer a convincing scenario.
- Brand Phishing – The attacker imitates another company, organization or agency that provides a product or service to the target—this is typically an attempt to steal credentials.

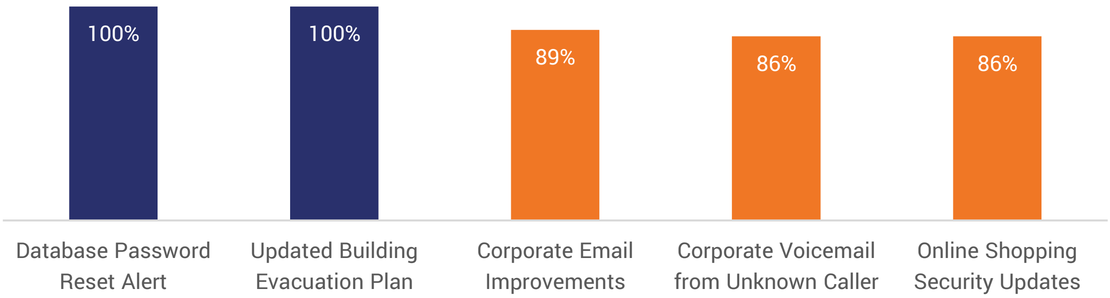
A phishing attack works as soon as it fools the target into believing it's authentic. From there, the desired action can take shape in myriad different ways, it could involve sending the victim to a website to harvest credentials, the email could contain a malicious payload. There's no shortage of possibilities. But the one thing that 99% of these phishing attacks have in common is they play on our emotions.

The emotions they're playing on seem to have shifted recently though. According to Cofense – which runs an education simulation called PhishMe – while urgency, fear and curiosity have historically been the leaders, recent initiatives to improve cybersecurity awareness and education have blunted some of the more mature phishing tactics. Additionally, as personal and professional email mingle, employees are increasingly likely to be victimized by a personal phishing attack while at work.



Plenty of research backs this up, too. In a recent Wombat Security study that looked at data from hundreds of corporate phishing simulations, the most successful phish were still the ones that stoked those emotions. Let's take a look at some of the most successful phish from Wombat's phishing tests.

Most Successful Corporate Phish



Finally, let's look at some of the most common words that appear in the subject lines and bodies of phishing emails. Unsurprisingly, a lot of these words trigger an instant, emotionally motivated response.

Subject Lines	Body Copy
✔ Payment (13.8%)	✔ Delivery (12.1%)
✔ Urgent (9.1%)	✔ Mail (11.8%)
✔ Request (6.7%)	✔ Message (11.3%)
✔ Attention (6.1%)	✔ Sender (11.2%)
✔ Important (4.8%)	✔ Your (11.2%)
✔ Confidential (2.0%)	✔ Returning (7.6%)
✔ Immediate Response (1.9%)	✔ Failed: (7.6%)
✔ Transfer (1.8%)	✔ Invoice (6.9%)
✔ Important Update (1.7%)	✔ Images (6.6%)

Phish are email-based attacks, but are all email-based attacks phishing?

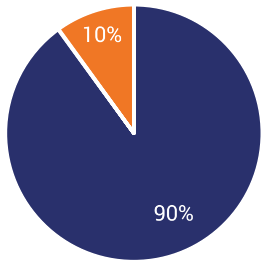
This question has troubled man for ages. Or at least since about 1997. The answer depends on your definition of phishing. If you define phishing as an end, then no. But if you define phishing as a means to an end, then the answer is yes.

Almost every type of email-based attack needs to fool the target into opening it and taking the intended action – whether that's infecting their system with malware or just stealing credentials. Ergo, phishing. The vast majority of email-based attacks actually don't contain malware though. 92.4% of malware is delivered by email, but just one in ten malicious emails contain malware.

No Malware

- Impersonation
- CEO Fraud
- Whaling
- SpearPhishing
- Credential Theft
- W2 Scams

Email Attacks

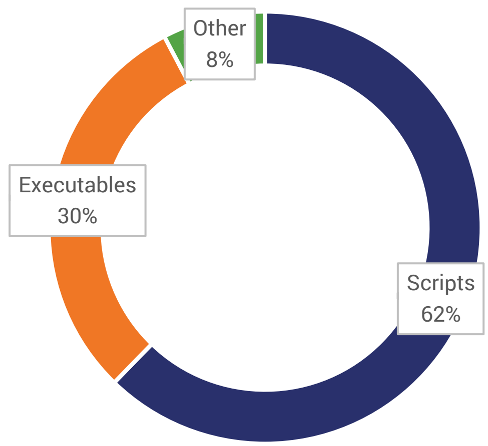


Malware

- Viruses
- Worms
- Ransomware
- Adware
- Trojan Horses
- Spyware

The vast majority of non-malware attacks fall into the three categories we described above—CEO fraud, Spearphishing or brand phishing. Whaling is a specific type of Spearphishing that targets high-level executives at a company. That differs from CEO fraud in that it's aiming to trick those executives as opposed to impersonating them.

Payload Type

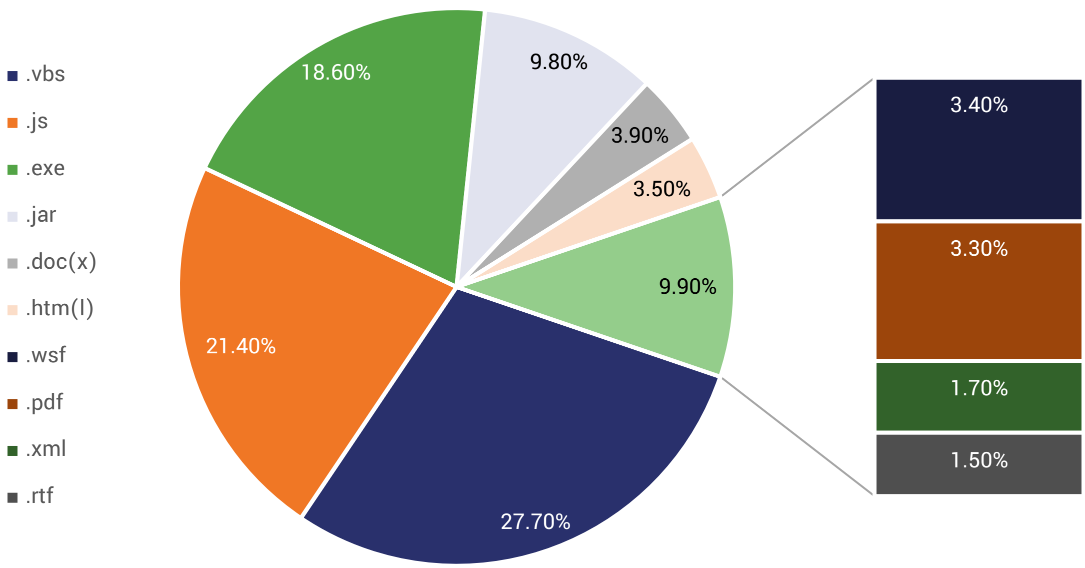


When an email's payload is malicious, it's almost always a script, typically Visual Basic Script or Javascript, which comprise just under 50% of malicious payloads.

This makes a lot of sense given their ubiquity. As we discussed before, the best phish imitate well-known companies and services because they give the criminals behind the phishing scheme the best chance of success.

If Adobe is one of the most widely used programs in the business world, imitating Adobe gives you a bigger pool from which to phish. Remember, the entire point of all that social engineering is to make the email believable enough that someone will take the intended action, whether that's entering credentials or opening a file.

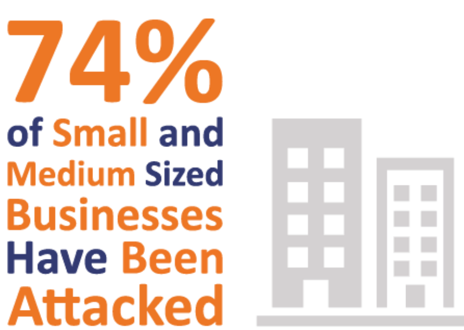
Most popular malicious payloads by file type



Finally, these malware-based phishing attacks oftentimes take advantage of other weaknesses in organizational security. Specifically, many of them count on the fact that your organization probably isn't patching regularly. Of the successful malware-based phishing attacks carried out in 2017 many also capitalized on outdated software. It goes without saying that your organization needs to stay on top of software updates to avoid exposing itself to any unnecessary risks.

Most commonly exploited outdated software

Adobe PDF	Adobe Flash	Java	Microsoft Silverlight
22%	21%	12%	9%
Down 29%	Up 75%	Up 50%	Down 47%



Stopping the Phish – Best Practices for defending your organization's email

There's no silver bullet – savvy organizations use multi-layered defenses including SPF, DKIM, DMARC, S/MIME Certificates, education, & spam filters

We've addressed the scope of the problem and identified some of the most common tactics of successful phishing scams, now let's talk about how to mitigate them. Ideally, if you configure everything correctly and set the right security policies you'll be able to stop the majority of these phish from getting delivered in the first place. But, as the research has borne out time and again: your employees are always going to be your biggest threat. Not necessarily out of malice, mostly just out of ignorance of best practices or simple negligence. So, training them will be of the utmost importance. Remember, technology doesn't get phished—people do.

But before we get to that, let's discuss how to secure your email servers and set up the correct policies and checks.

What technical safeguards are organizations using?

97%	47%	44%	31%
Email/Spam Filters	Advanced Malware Analysis	Outbound Proxy Protection	URL Wrapping

Let's start with the low-hanging fruit. Every email client, server, etc. is different so there is no one-size-fits-all solution that can be offered. Instead we'll focus on the concepts. Most of these are common sense steps, but for the sake of thoroughness, we'll go through them anyway.

Invest in a quality antivirus program

Many antivirus programs come with built-in mail filters and scan files and websites for known malware or other security risks. Find one that does both. Ideally you should be able to set it up with your mail proxy/relayer so it can scan emails before passing them along to your organization's inboxes. A good antivirus might be able to catch what your server software and system security may have missed.

Your entire organization should already be using an antivirus program, but not everyone is able to maximize their value. So, spend some time under the hood, figure out what additional features it may have and how you can leverage those to help better defend your company's email. Then train your employees to heed it. Even the best antivirus program in the world isn't much help if the user just ignores it.

Spam Plugins/Filters

Using the spam filter that came with your organization's email client is typically a good start, but depending on how stringent it is, you may also want to look for a third-party plugin. A couple good examples are SpamBully and MailWasher. Most of the time the default setting for these filters is set to "no automatic filtering." Obviously, that's dangerous, but be careful going up in protection level because you may end up filtering out legitimate email, too. It's best to adjust the settings incrementally so that you can gauge their effectiveness before making any drastic changes.

Blacklists and Whitelists

Having a living, breathing blacklist of banned addresses is vital to email security across your organization. You should be maintaining that list by:

- ✓ Domain
- ✓ Email Address
- ✓ IP Address/Range

If you don't want to manage the blacklist yourself, there are also Spam blacklist authorities that offer subscriptions. When an offender is placed on one of these lists, they have to make a formal appeal to the authority to be delisted.

Whitelists on the other hand tell your servers and filters what email should always be allowed through. Much like your blacklist, your whitelist should be maintained by:

- ✓ Domain
- ✓ Email Address
- ✓ IP Address/Range

SMTP (Simple Mail Transfer Protocol)

SMTP has features that can help to defend against spoofing within your own organization. Most organizations use SMTP for internal email, so it's critical that you enable its authentication functionality on all of your organization's email servers. SMTP is fairly easy to configure and then store the settings on your organization's devices.

Rules are your friends

Setting up custom rules is one of the best features of many email clients, enabling you to filter mail as desired and better organize your inbox. Allowing your employees to create their own rules can help improve organization and work flows but making them at the administrative level can also help better defend your organization. You should train every employee to instinctively flag spam or malicious email, this ensures that it gets added to the blacklists and can help better inform any rules that need to be made at the administrative level.

Now that we've covered the easy stuff, let's get into some more advanced strategies to help defend against phishing, and email attacks in general. It's worth noting that aside from the S/MIME and employee education sections, the other strategies – SPF, DKIM and DMARC – discuss mechanisms that help your email's recipients verify that email actually came from your organization. In other words, they help protect you against being imitated by phish.

Email Security Best Practices – Advanced Strategies

- S/MIME Certificates
- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- DMARC & Reporting
- Employee Training/Education

Catching Phish with S/MIME

S/MIME stops email spoofing and protects against CEO fraud, whaling and spearphishing. It also helps ensure your email reaches its intended destination. One of the most pernicious effects that phishing has had on the internet in general is that it's made most email clients especially finnicky about what they'll deliver. In fact, according to a Return Path study, only 79% of legitimate email actually makes it to the inbox.

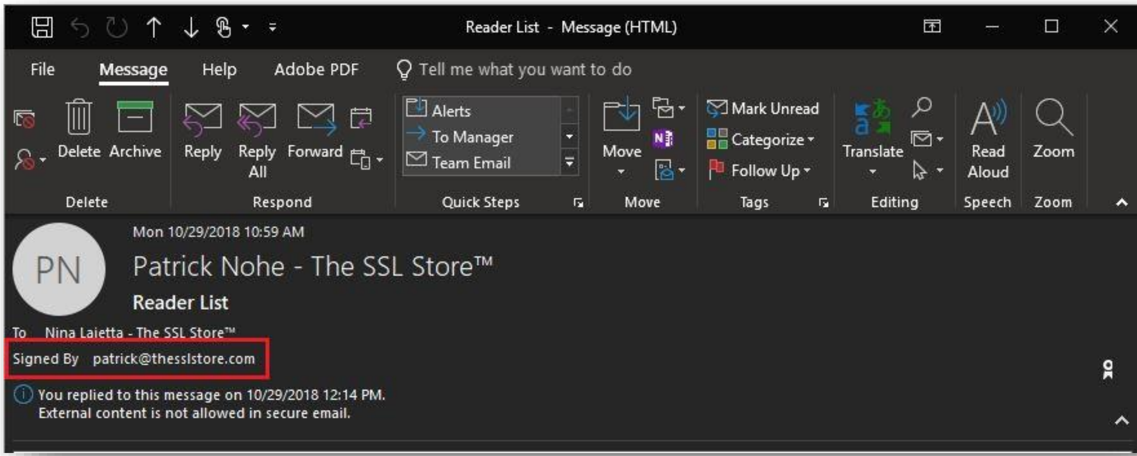
That means more than one out of every five legitimate emails gets filtered out.

That makes email signing certificates doubly beneficial. Because not only do they help ensure outgoing mail makes it to its intended destination, they also provide a much need layer of protection internally for your entire organization by asserting sender identity in the form of a digital signature.

79%

…of email actually gets delivered

Because email signing certificates are validated by a trusted certificate authority – one with trusted roots – the digital signature affixed to emails by a trusted S/MIME certificate confirms the identity of the sender to the recipient. Just like with websites in general, asserting identity is one of the only ways to give your customers, clients or employees confidence about your identity.



It's especially useful for emails sent within your own organization. The debacle at Mattel would have never happened if the organization was using S/MIME certificates. If every employee has an S/MIME (Secure/Multi-Purpose Internet Mail Extensions) certificate, and it's mandatory to sign all email – you're going to be able to stamp out CEO fraud and other forms of phishing that imitate certain departments or personnel.

If an email comes from within the company and it's not signed, it's immediately suspect. This takes a lot of the human element out of the decision-making process and replaces it with a simple binary. Signed? Trusted. Not signed? Scrutinize.

Why isn't S/MIME more prevalent?

S/MIME's Achilles heel has historically been deployment. For S/MIME certificates to work optimally, everyone in the organization needs one. Historically, that's meant installing certificates device by device. One at a time.

And for many organizations, that's made S/MIME seem like more trouble than it's worth.

There's a solution to that now though. Sectigo is the first Certificate Authority that has created a Zero-Touch S/MIME platform that automates the entire lifecycle of your S/MIME certificates. This means that an IT manager or someone from your security team doesn't have to install every certificate individually. It means anytime an employee joins the company or leaves the company you don't have to go through a protracted process to get them a new S/MIME certificate or revoke their old one.

Instead, Zero-Touch S/MIME gives you control over requisition and revocation of email signing certificates through a single interface by integrating with your organization's Active Directory. The process is completely invisible to users—it all happens behind the scenes. A far cry from having to install one on your mail client and add it your directory manually.

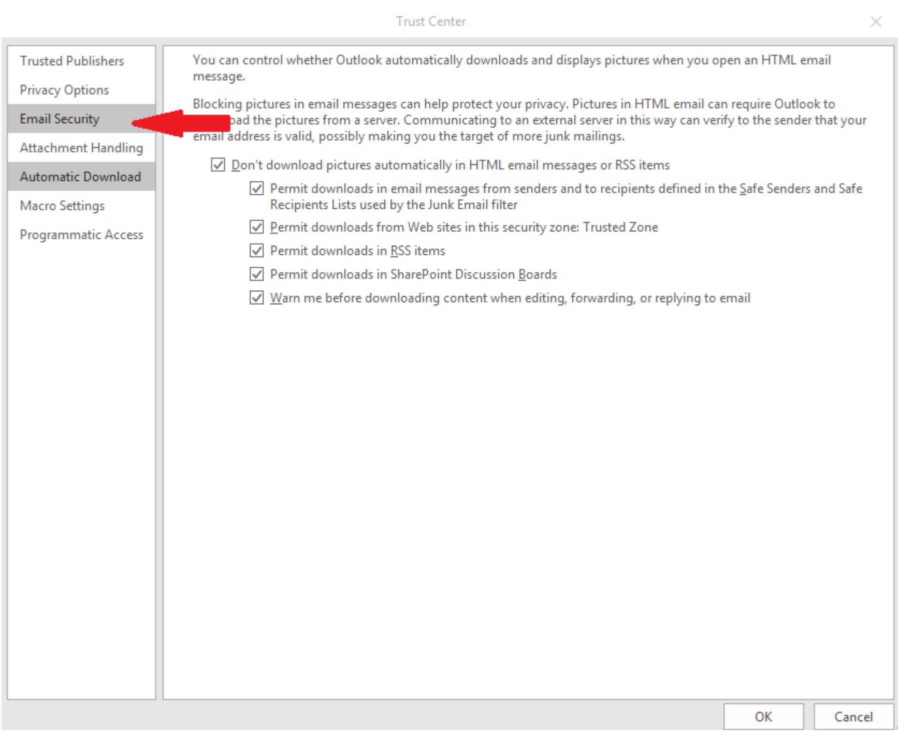
This is the easiest, most cost-effective way to manage S/MIME certificates.

But, if you want to do it the old-fashioned way, here's what you have to look forward to.

Installation of S/MIME certificates is a straightforward process. But it can be tedious. Let's take a look.

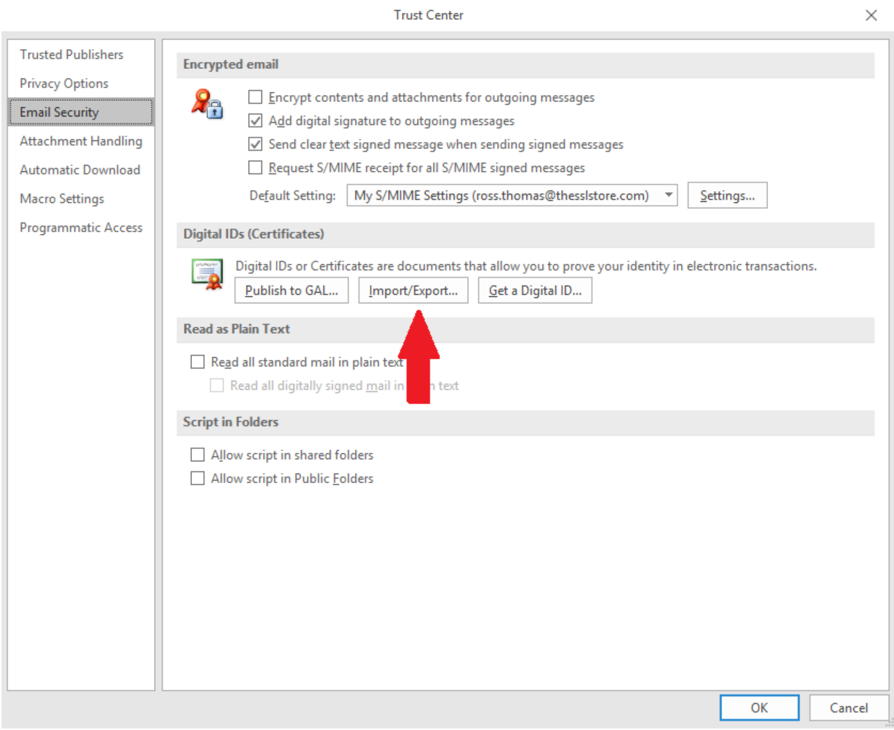
Assumptions:

- ✔ Windows 7+
- ✔ Outlook 2016
- ✔ Possession of a proper security certificate file (.crt)

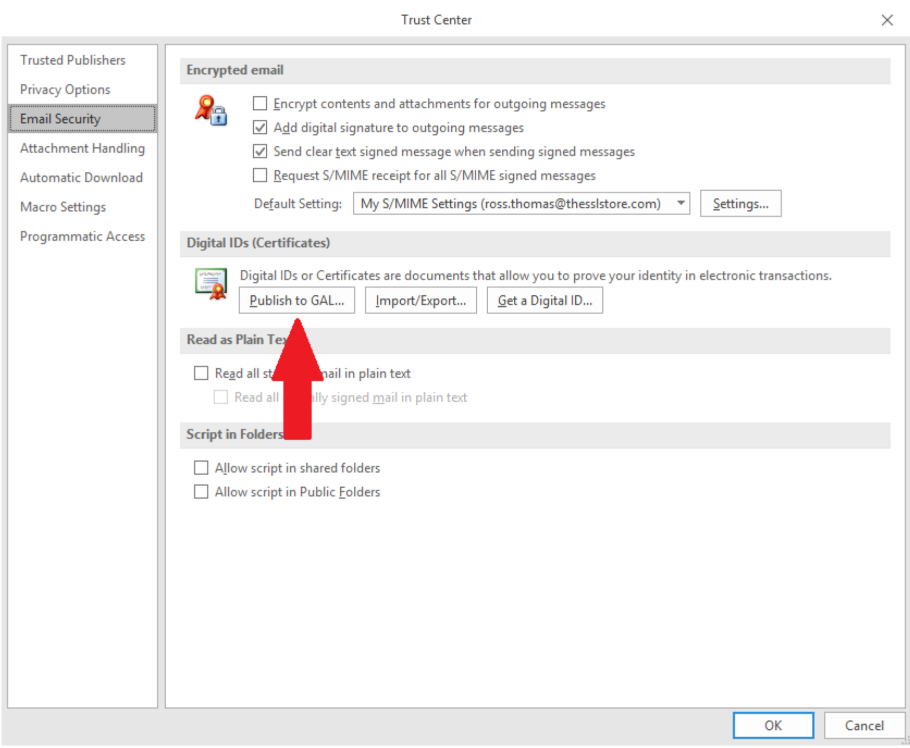


Execution steps:

- Open Outlook 2016
- 'File'->'Options'->'Trust Center'->'Trust Center Settings'
- Trust Center window will appear
- Select 'Email Security' in the left menu options

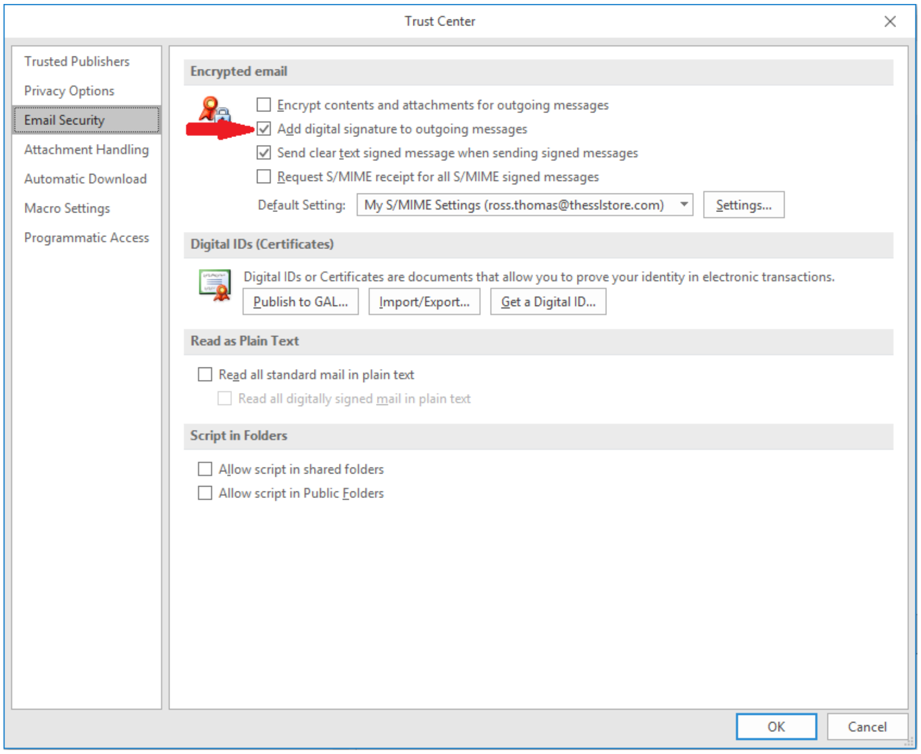


- Select 'Import/Export' and the window will appear
- Browse to certificate and enter appropriate password (if applicable)
- Select 'OK' and the certificate will import
- Select 'Publish to GAL'
- There will be notification that this has completed

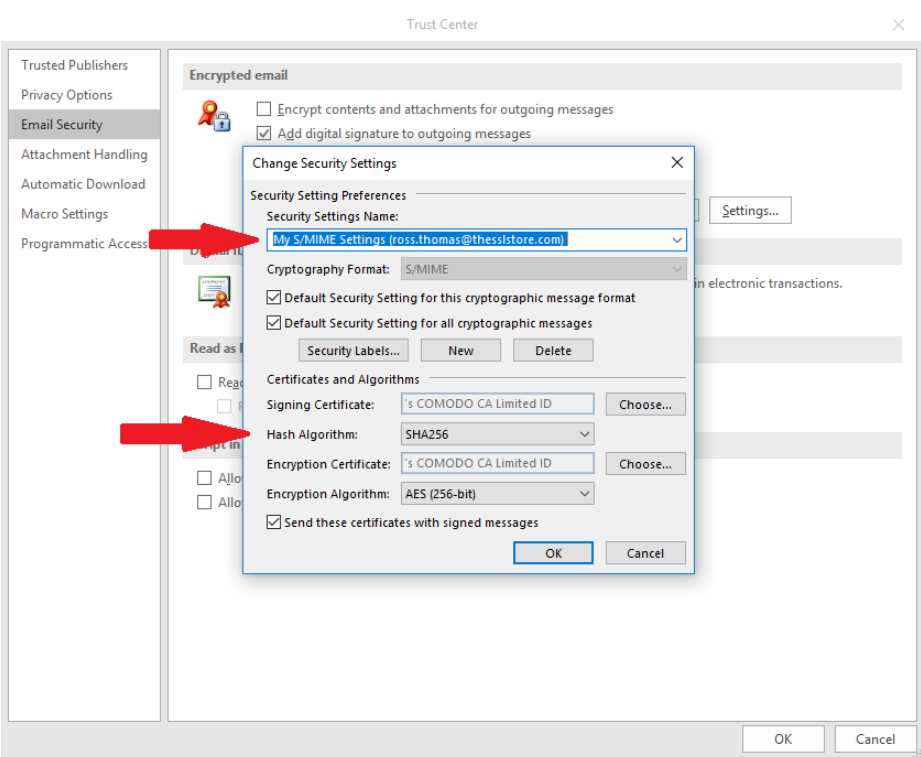


Configure certificate for email client

- Open Outlook 2016
- Go to the trust center settings outlined in the previous section
- There is an optional checkbox for 'Add Digital Signature for Outgoing Messages'
- This will sign every email generated for that particular email domain



- Select 'Settings'
- Under 'Security Settings Name', make sure the correct email domain is selected
- In the 'Certificates and Algorithms' section, make sure the 'Hash Algorithm' is higher than 'SHA1' (selected by default). 'SHA256' is acceptable by most mail services/exchangers so that should be sufficient.
- Select 'OK'

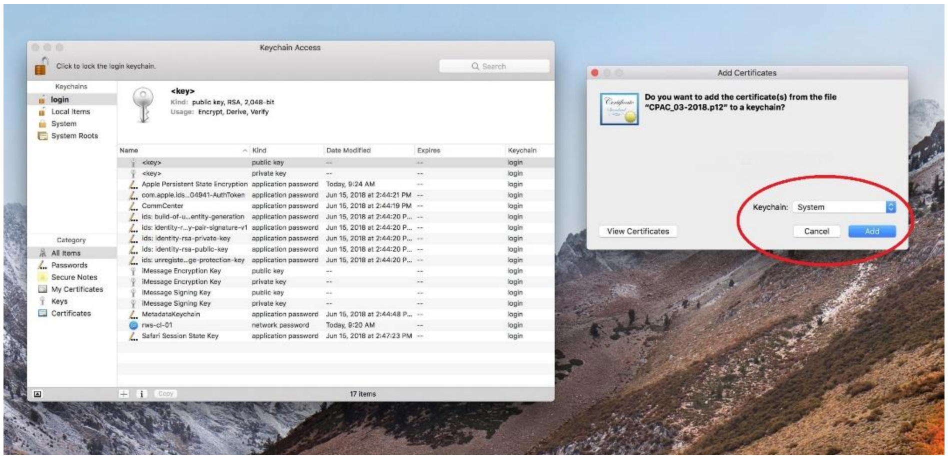


- Select 'OK' to close the Trust Center.

Now let's look at how to configure S/MIME certificates on macOS.

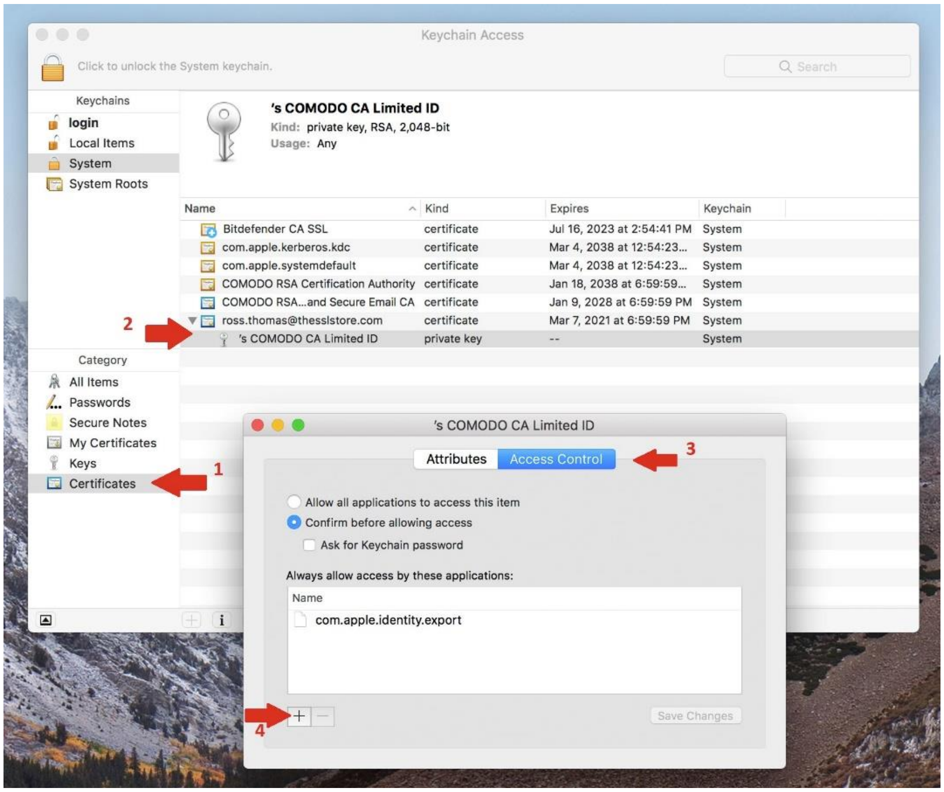
Assumptions:

- ✔ OS X version 10.5.8 or later (this includes any macOS version)
- ✔ Outlook 2016 for Mac
- ✔ Possession of a proper security certificate file (.p12)

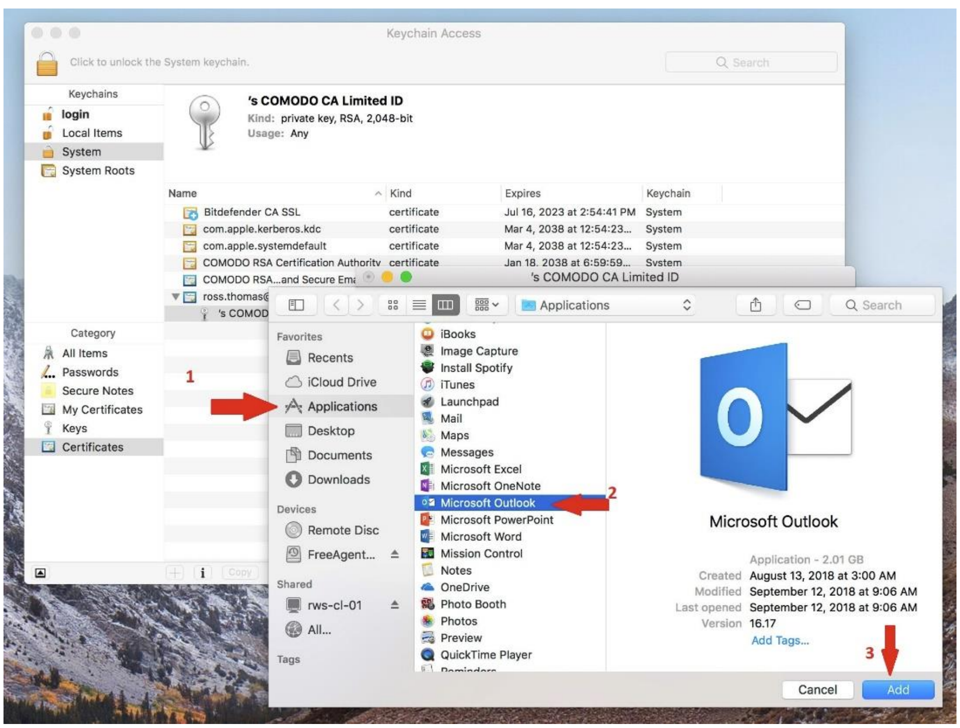


Execution Steps:

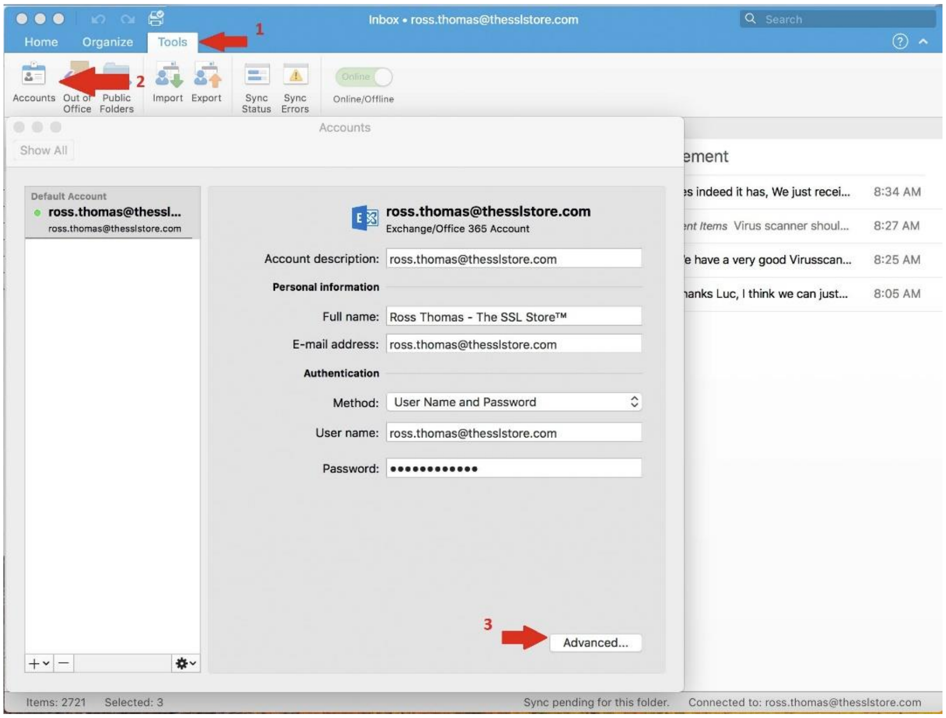
- Double click your .p12 certificate to add to 'Keychain Access'
- There will be a prompt to 'Add Certificates'
    - Keychain = 'System'
- Click 'Add'



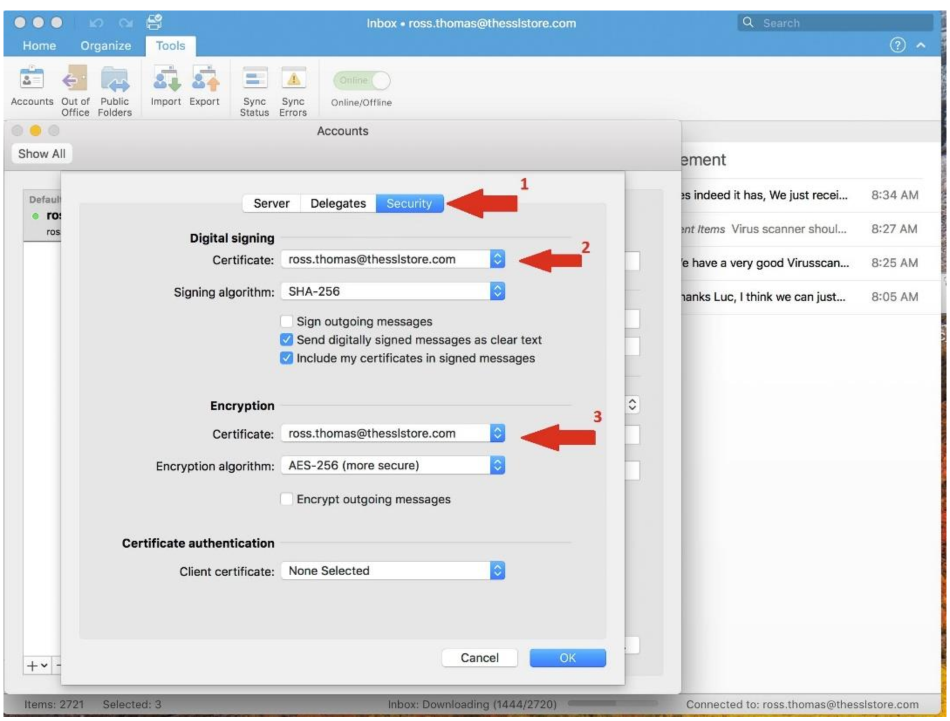
- Under ‘Category’, click on ‘Certificates’ to populate the current certificates in the view pane
    - Expand the certificate that was just added, and double click the ‘Private Key’ associated
    - Select the ‘Access Control’ tab to show what applications are allowed to have access to the key
    - Ensure that the radio button is selected for ‘Confirm before allowing access’
      Note: Optionally, you can select ‘Ask for keychain password’ for a little further security
- Click the ‘+’ button to add an application



- There will be a prompt to associate the private key to
    - Select ‘Applications’ to get a list of the computer’s applications
    - Select ‘Microsoft Outlook’ to allow access to the certificate
- Select ‘Add’

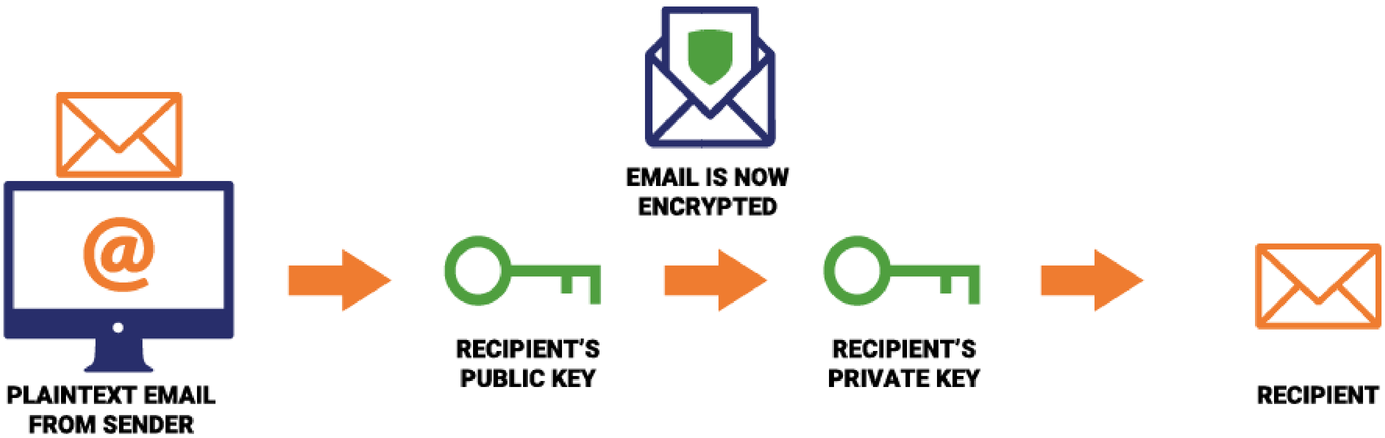


- In Outlook, select the ‘Tools’ tab up top
    - Click on ‘Accounts’ and make sure the correct account is selected
- Click the ‘Advanced’ button in the lower right of the pane



- Click on the ‘Security’ tab in the ‘Advanced’ window pane
    - Under ‘Digital Signing’ -> ‘Certificate’, select the dropdown and pick the correct certificate (which the private key is associated to)
    - Check the box to automatically ‘Sign outgoing messages’, ‘Send digitally signed messages as clear text’ and ‘Include my certificates in signed messages’
- Under ‘Encryption’ -> ‘Certificate’, select the dropdown and pick the correct certificate (which the private key is associated to)
    - *Note: Leave the box to automatically ‘Encrypt outgoing messages’ unchecked*
    - *Note: Set the certificate for ‘Certificate Authentication’*

A quick note, the reason we're not encrypting all outgoing mail is that it could make the messages unreadable for some parties. You would need to have your recipient's public key in order to encrypt the email in a way that would make it decryptable to them.



You'll still have an option to encrypt sensitive communication when you send each individual email, or any email within your own organization/network, but categorically encrypting all outgoing mail is ill-advised.

Certificate Management made simple

Now that you've set your entire organization up with email signing certificates, you've got another issue to deal with: managing them all. If you're only dealing with a handful of certificates this might be no problem at all. But at scale it can be nightmarish. Historically, certificate management has involved the copious use of spreadsheets and aspirin. Don't do that. Sectigo's Zero-Touch S/MIME is an application that's part of its larger Sectigo Certificate Manager, which is an all-in-one platform for managing digital certificates. Not just S/MIME, but SSL/TLS client and server certificates, even Code Signing.

We can't stress enough how important it is to invest in a quality certificate management platform like **Sectigo Certificate Manager** or **DigiCert's Cert Central**. A good certificate management platform gives you complete visibility over your entire organization's certificates

A single interface enables you to automate everything, keep track of certificate lifecycles and receive notifications when certificates near expiration. If you'd like to learn more about Certificate Management, please take a look at our Certificate Management whitepaper.

And as always, call us for a free consultation. We've been helping businesses and organizations with their certificate management needs for ten years. We can help you, too.

Download our Whitepaper

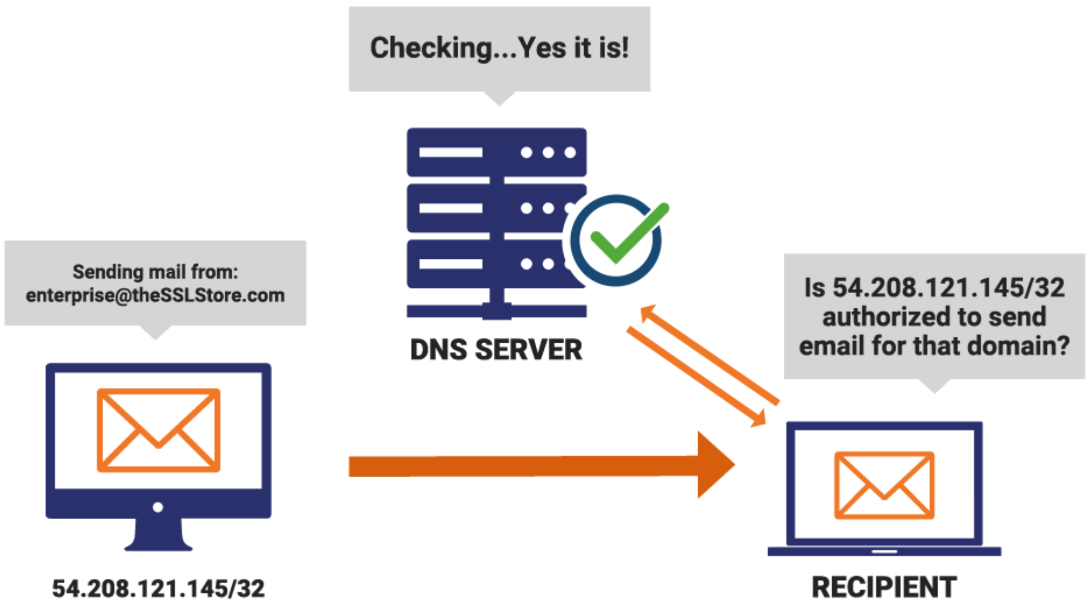
Setting up a Sender Policy Framework (SPF)

SPF or Sender Policy Framework is a protocol referenced by a DNS entry, which indicates the valid IP addresses that are authorized to send email from a given domain. This is incredibly important in discerning whether an email is legitimate. If you receive an email from an American vendor, you want to verify that it originated from that vendor's network and not from, say, Eastern Europe.

So, SPF is referenced by a DNS entry that indicates specific IP addresses, blocks of IP addresses or other domain names, for example all the following would be valid entries:

- IP Address with CIDR Notation: 54.208.121.145 /32
- IP Address Block with CIDR Notation: 199.127.232.0 /22
- Domain names: domainname.com

If an email comes through from an IP address that's listed in the DNS' SPF record, then it's considered compliant and gets through. If an email originates from an IP address that's not listed, it isn't trusted and will be flagged as such. Again, this helps take a lot of the guesswork/human element out of the decision-making process.



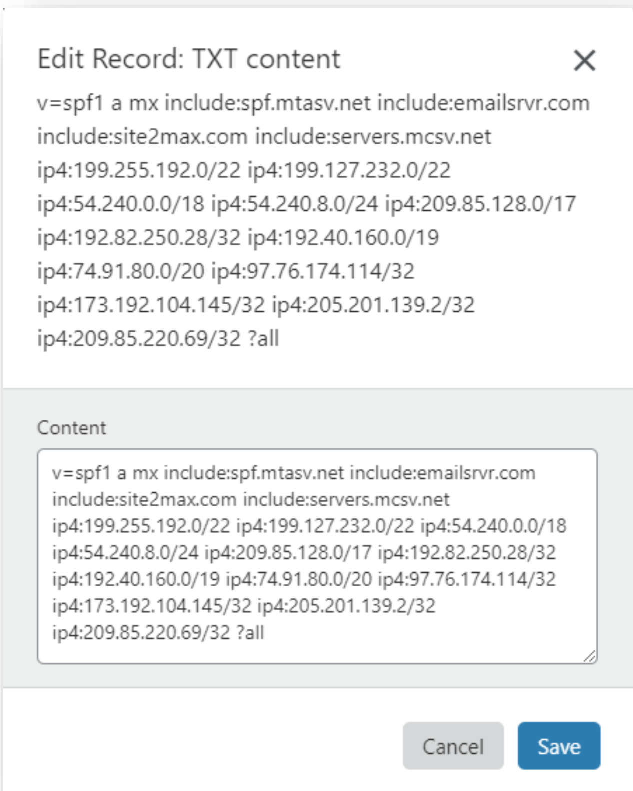
SPF is more for your outgoing mail than your incoming mail because it helps inform your email's recipient whether they can trust it. It has the fortunate side effect of further layering your email security, given that it can sniff out impostor emails that purport to be sent from within the company. SPF's primary benefit comes from helping other organizations determine that your emails are legitimate. This helps with your DMARC score, as we will discuss in a few sections. Between signing your email and ensuring the domain or IP address they originate from is listed in your SPF record, you'll have very little trouble making sure your email arrives at its intended destination.

For businesses that own their own mail server or that use a third-party service, setting up SPF should be simple – requiring just a single entry. Unless the email is going through some kind of mail exchanger, in which case you'll also need to list the IPs for the intermediary or mail exchanger.

If you're an organization that has email sent from all over the place – for instance, from a customer service platform like Freshdesk and a marketing automation platform like Marketo – SPF is going to require a little more effort because you'll need to set up individual entries for each email domain. Suffice it to say, SPF isn't necessarily a 'set and forget' function. It takes time and tracking to fine tune your SPF DNS entry to optimize your organization's trusted email delivery.

SPF entries are publicly available, so let's look at The SSL Store's.

Ok, now let's look at the entry itself and break down some of the individual mechanisms that can define the sets of hosts that are authorized to send email from a given domain.



a – This will match the domain's 'a' record

mx – This will include the IP(s) of a domain's mail exchanger record

These first 2 parameters are typically standard but can be fine-tuned to put more restrictions about what is acceptable.

include – There are a series of 'include:' statements followed by domain names which list acceptable mail originators for this email domain. This will include the DNS lookups mentioned earlier in this eBook.

ip4 – This series of 'ip4' listings is specific IPs and IP blocks. Note: IPv6 can also be specified but the internet is, apparently, still not ready for widespread IPv6.

all – This matches any host, it's placed at the end of the SPF record and acts as a "catch all" for any senders that don't match the other mechanisms listed ahead of it.

You can attach qualifier symbols to any of these mechanisms to further modify them.

Here is what the qualifier symbols mean:

- *+ Pass an IP that matches IP*
- *- Fail an IP that matches IP*
- *~ Run the SPF rules against email but don't enforce. Flags email as "fail" but allows it through*
- *? Neither pass nor fail. Essentially disables SPF*

Additional mechanisms

There are a few additional mechanisms that don't appear in the example we just used. We'll list them here for your reference:

IP6	Checks that the email originates from a single IPv6 address or an IPv6 network range
PTR	Calls for a reverse DNS query to match the sender's IP to the host name it resolves to
exists	Simply checks DNS to see if the domain exists

By adding your SPF entry as a TXT record in your public DNS zone, you're effectively preventing an attacker from imitating you and your domain name. Granted, if a mail server isn't checking SPF records, the mail will continue through unabated. But that's on them. We mentioned earlier that phishing is a crime with two victims: the one being imitated and the one being duped. SPF helps protect against the former.

Additional SPF Tips

- Keep your SPF records as simple as possible, don't put any more hosts in your SPF records than you need to.
- Use the "Include" mechanism sparingly, avoid nesting them where possible and never use so many that you go over the 10-lookup limit.
- When specifying blocks, use ranges between /30 and /16. Avoid anything between /1 and /15. The higher the number after the slash, the smaller the range.
- Never create a record using +all, only use ~all or -all.

Add even more trust with DomainKeys Identified Mail

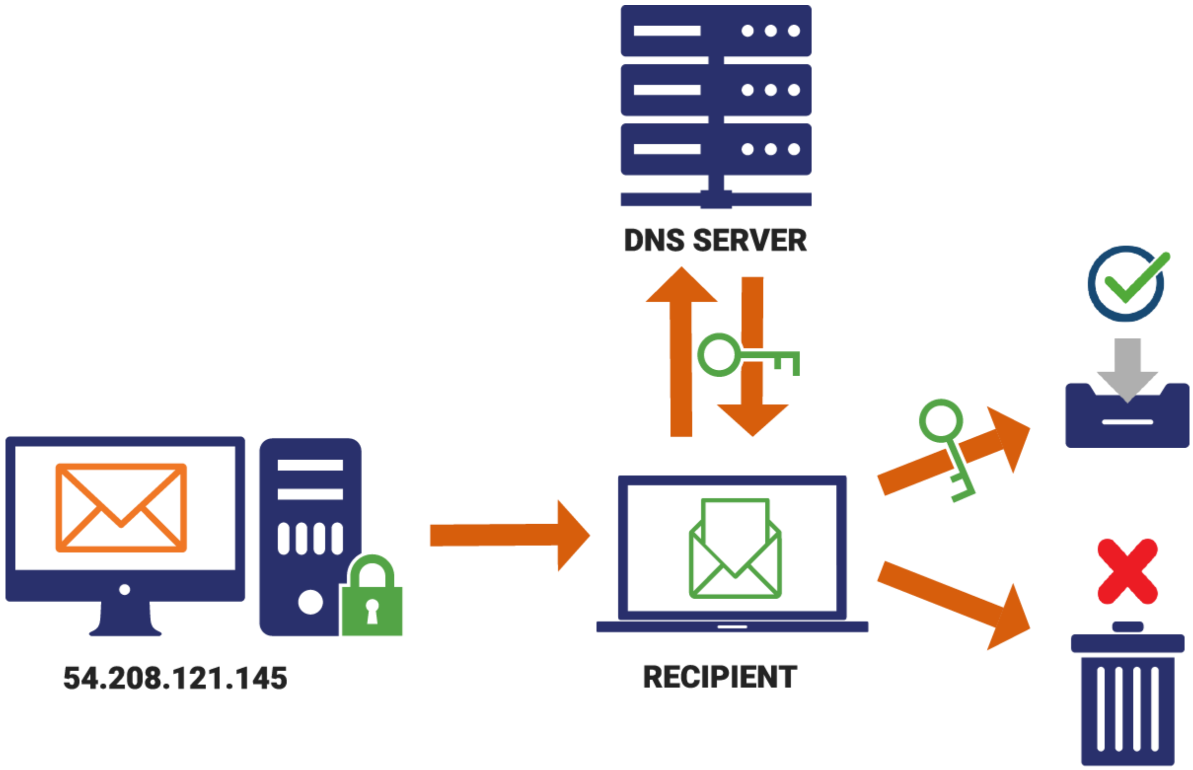
DKIM or DomainKeys Identified Mail is a perfect complement to SPF. Sender Policy Frameworks are ideal for smaller companies with their own email servers and only a handful of IP addresses or ranges from which their email originates, but at scale– or when using a third-party provider – SPF can run into some problems.

Especially if an attacker is sending email from a spoofed address using the same IP addresses as you.

Take for instance AmazonSES, which has millions of users and can send millions of emails daily. Specifying the dozens and dozens of allowable IP addresses might not be enough to dictate who can send what and from where on AmazonSES. Tons of people use the service, so the ability to spoof emails when both parties use AmazonSES renders SPF fairly useless.

Enter DKIM.

DKIM isn't very complicated conceptually or functionally. And much like SPF it involves updating your DNS records. This time you're going to be adding a cryptographic key that can be used to sign emails and validate that they are authorized to emanate from that server. Let's start with how it works, and then we'll move on to how to set one up.



Conceptually, you're adding a DKIM public key and a selector, which is used as an additional name component to help give differential DNS query names. When an email is written and sent, the server will use the associated DKIM public key to sign it. Upon receipt, the other mail server uses the selector to check the signature against what's listed in the DNS record. Provided they match, the DKIM is validated and the email reaches its intended destination.

DKIM, like SPF, protects against phishing on both fronts as it helps prevent attackers from imitating an organization while also helping the company that is being attacked identify imposter emails. Not only that, but DKIM uses a checksum to ensure that the content of the email has not been modified in transit, which further aids in ferreting out the phish.

Setting up DKIM

Setting up DomainKey Identified mail is a very straightforward process owing to the fact that most of the work has already been done for you. Most mail services (Office.com, Rackspace, AltMail, etc.) have a section dedicated to DKIM (sometimes it may be listed as "Sender Authentication" or something along those lines).

Whatever service you're using will generate a unique cryptographic public key or signature for your email domain. You'll need to copy the key into a TXT record in your public DNS zone. The selector goes in the DKIM signature header field. Here's an example:

v=DKIM1; k=rsa; p= HeYxdz0GCSqGSIb3DQEBAQUAA4GNADCBc/s77MZPKk2hAcP5CfxsgZJiQKBg QClfSa9MKd6KtasdpZv2sGhKcNFEGzhkk1yrEHonXNBJPAtXawYbALk8+jpse4 A3cOubP5v9WVE1cAIuBJ2JSNPbljfuFLc0l+5v9WVE1cVRXDum+BLxy

SPF and DKIM work well in tandem and are absolutely critical to getting the most out of DMARC, which we'll cover now.

Additional DKIM Tips

- Use 2,048-bit keys. This is the industry standard, anything smaller is not secure.
- Rotate keys regularly. The longer a key is active, the longer attackers can attempt to crack it. Rotate keys at least once per year, more if you send a high volume of emails.
- Make sure that your Email Service Provider (ESP) doesn't use the same key for all of its customers—you need unique keys.
- If you generate bounce messages, make sure you're signing them using DKIM.

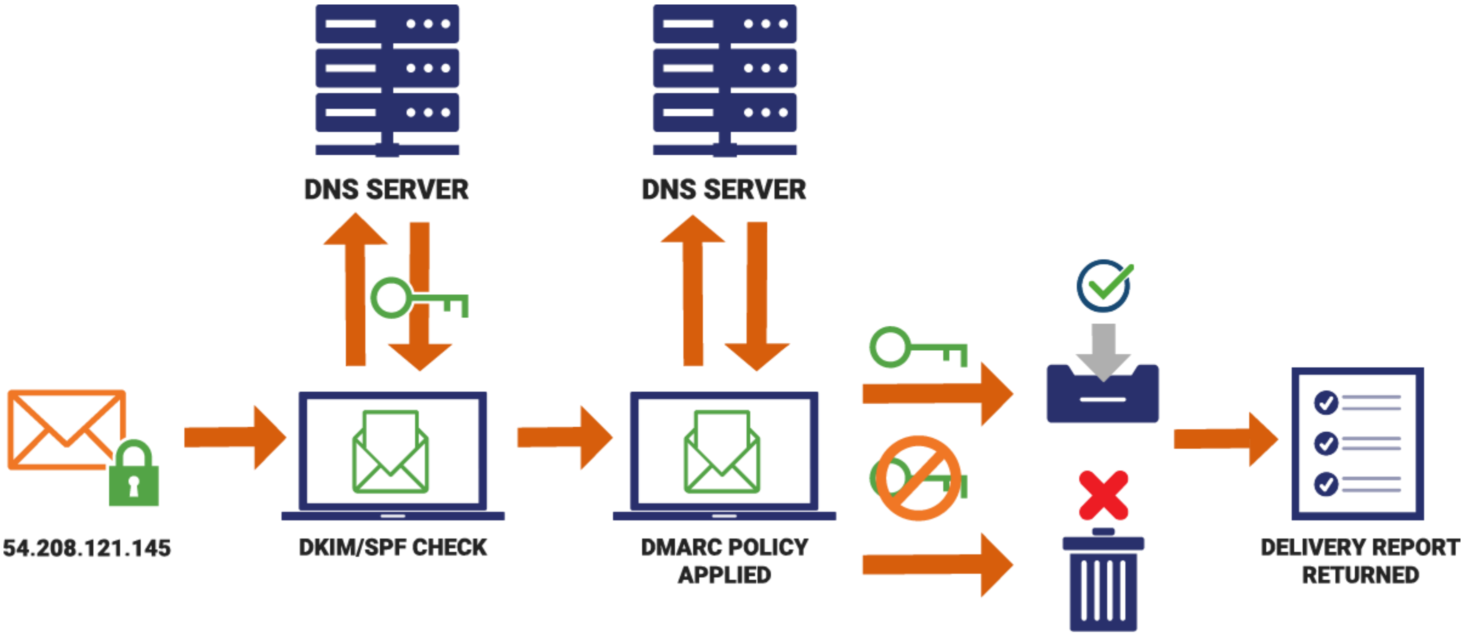
Domain-Based Message Authentication, Reporting and Conformance (DMARC)

DMARC or Domain-Based Message Authentication, Reporting and Conformance is an email authentication, policy and reporting protocol. It's designed specifically to help detect and mitigate email spoofing and forged sender addresses, which are commonplace with both phishing and spam. DMARC is built on top of SPF and DKIM. That's why we covered those first.

Like both DKIM and SPF, DMARC is facilitated through DNS records. From a top-level perspective, DMARC:

- Specifies the mechanism (SPF, DKIM or both) employed when send email from that domain.
- Specifies how to check the "From:" field presented to end users.
- Specifies how the receiver should handle failures.
- Provides a reporting mechanism for any actions performed under the aforementioned policies.

Setting up your company's DMARC account with all your email domains will offer some peace of mind and helps with evaluating the overall status of your email flow. You've already set up SPF and DKIM, DMARC is recording the results of both other protocols whenever an email originates from one of your domains. It also allows gives you more granular control when dictating how to handle failures for either, or both.



So, let's figure out how we want failures to be handled and create a DMARC DNS entry.

We're currently on DMARC version 1, so you're going to need to specify that (v=DMARC1) at the beginning of the DNS entry.

The policy, or *p*, is where the real decisions start to get made. This is what determines what happens with the traffic that fails either DKIM, SPF or both. The options are pretty straightforward:

- *P=none – No action will be taken. There will only be record of the failure.*
- *P=quarantine – The email is flagged as spam and subject to the recipient's spam policies.*
- *P=reject – The email is flagged as malicious and dropped by any exchanger, domain or inbox client listening.*

Let's take a look at a couple of other basic options for reporting:

- *rua – This dictates where aggregated email reports should go. Aggregated reports show the number (volume) of messages and how they fared with SPF and DKIM. The destination is typically an email address. The DMARC services will often provide an email address to load in so that they can parse and arrange the data into something readable.*
- *ruf – This dictates where the forensic email reports should go. Forensic reports include more information on the SPF and DKIM failures to offer insight on what went wrong. The destination is typically an email address. The DMARC services will often provide an email address to load in so that they can parse and arrange the data into something readable.*

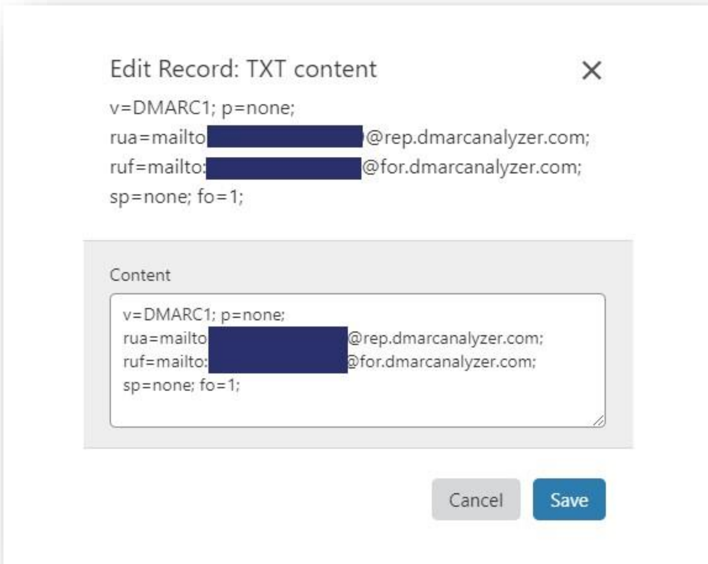
More DMARC Options

sp	Subdomain policy – like Policy (p), it has qualifiers: none, quarantine and reject.
pct	Percentage – indicates the percentage of failures to be reported. Values: 1-100.
adkim	DKIM Alignment – it has two qualifiers: relaxed (r) and strict (s). Strict requires exact domain match.
aspf	SPF Alignment – aspf has two qualifiers: relaxed and strict. Strict requires exact domain match.
fo	Forensic Option – dictates the conditions under which a forensic report should be sent out. Values: 4.

Forensic Options

There are four different values for the Forensic options mechanism, they dictate the conditions that require a report to be sent:

- *0 – Dictates a report must be sent if both DKIM and SPF fail.*
- *1 – Dictates a report must be sent if either DKIM or SPF fail.*
- *s – Dictates a report must be sent if SPF fails.*
- *d – Dictates a report must be sent if DKIM fails.*



A Practice Example

Much like with SPF and DKIM, DMARC requires you to create a TXT record in your public DNS zone. By now you know how to do that, let's look at one of The SSL Store's DMARC DNS entries.

Note: *We've obscured the address where our reporting goes for proprietary reasons.*

This is a fairly straightforward example. Let's go through each mechanism.

Version – DMARC version 1

Policy – In the event of a failure, no action will be taken but a record will be made.

RUA & RUF – The DNS entry dictates that reports be sent to a proprietary email account.

Sub-domain Policy – In the event of a failure, no action will be taken but a record will be made.

Forensic Options – Send a report in the event that either SPF or DKIM fails.

You should have a pretty solid idea how to put together the right DMARC DNS TXT record by now. Early on you may want to opt for more regular reporting with the maximum amount of information provided so you can start to get an idea as to the health of your email servers and your DMARC reputation. The better your reputation, the more of your emails get through and the less likely others are to fall for phish that imitate you.

Additional DMARC Tips

- Identifier Alignment, which is handled by the adkim and aspf mechanisms, is critical to your success when using DMARC. What this means is that when the mechanisms are set to "strict," the domain names to match what's listed in both the "MailFrom" and "Header From" fields. These are two different things. The "Header From" domain is visible in the "From:" field within the email itself. The "MailFrom" field is typically found in the "Return Path" message header.

The best defense against phishing is education

If you set your email servers up correctly, make use of SPF, DKIM and DMARC, and you've equipped every employee with an S/MIME certificate, you've done just about everything you can from a technology standpoint.

Unfortunately, successful phishing attempts usually don't compromise security systems, they compromise people. The human element is what makes phishing so dangerous. Even if you do everything correctly, a few emails are occasionally going to slip through.

> "The human element is what makes phishing so dangerous…"

And even if that doesn't happen, employees open their own personal email accounts on work computers all the time.

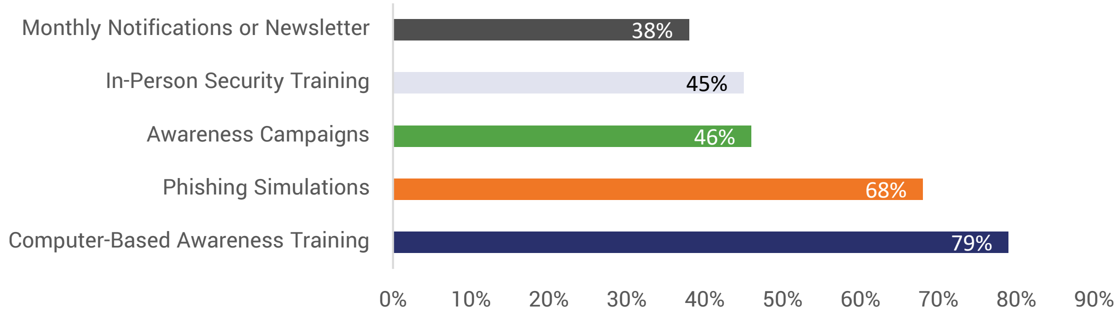
That's why education is so critical in defending against phishing and email attacks in general.

Let's start with some top-level ideas and then go through a few examples.

What are other organizations doing?

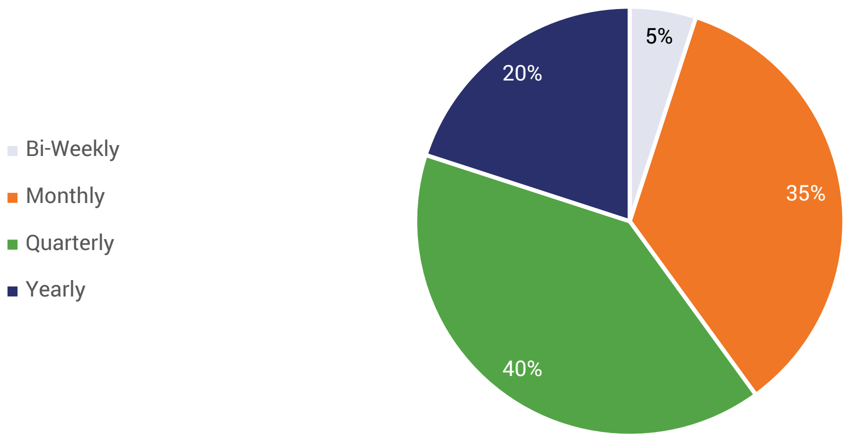
There's no shortage of good training material when it comes to organizations educating their employees about the perils of phishing. But before you decide on how to educate your personnel, let's take a look at what other organizations are doing.

What tools other organizations are using



Over two-thirds of the companies that responded to Wombat's security survey, 69%, also said they assess the risks posed by individual employees looking at a combination of their performance during training, proprietary risk assessments and violations of technical and administrative policies.

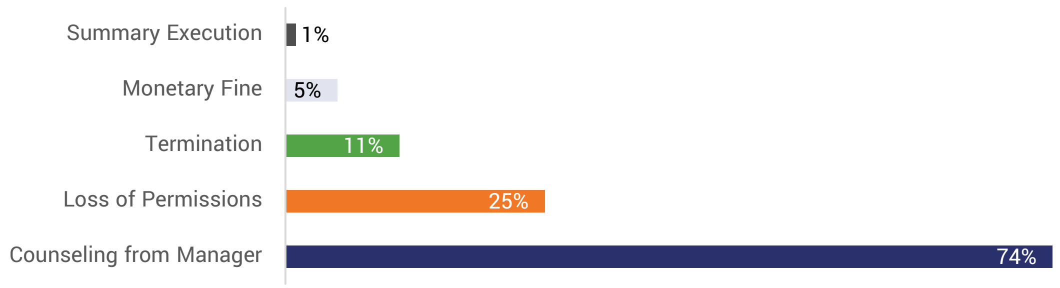
How often organizations train employees



Most organizations want to err on the side of caution and provide training either monthly or quarterly: anything more risks your employees tuning you out and anything less is borderline negligent. Generally, organizations see the best results between years one and two of their training program. It's important to revisit email security training regularly due to:

- Staff Turnover – According to the US Bureau of Labor Statistics, the average worker will hold ten different jobs before age 40. Employees come and go all the time, it's a fact of life. What you don't want is for an employee to be on the job for months before they ever get email security training. Ideally you should include some training in your organization's onboarding materials.
- Threats Evolve – Phishing, and cybercrime in general, are constantly evolving, constantly finding new ways to trick people. The training material you had two years ago likely isn't going to cover everything you need it to nowadays. So, it's important to constantly be updating your training curriculum to respond to recent trends and threats.
- People Forget Things - Some of your employees would have a hard time telling you what was discussed in the meeting they just walked out of, let alone be able to remember all the security information you threw at them six months ago. So, revisit the material often and try to ensure every employee has at least a working knowledge of how to handle suspicious email.

How organizations punish employees that get phished

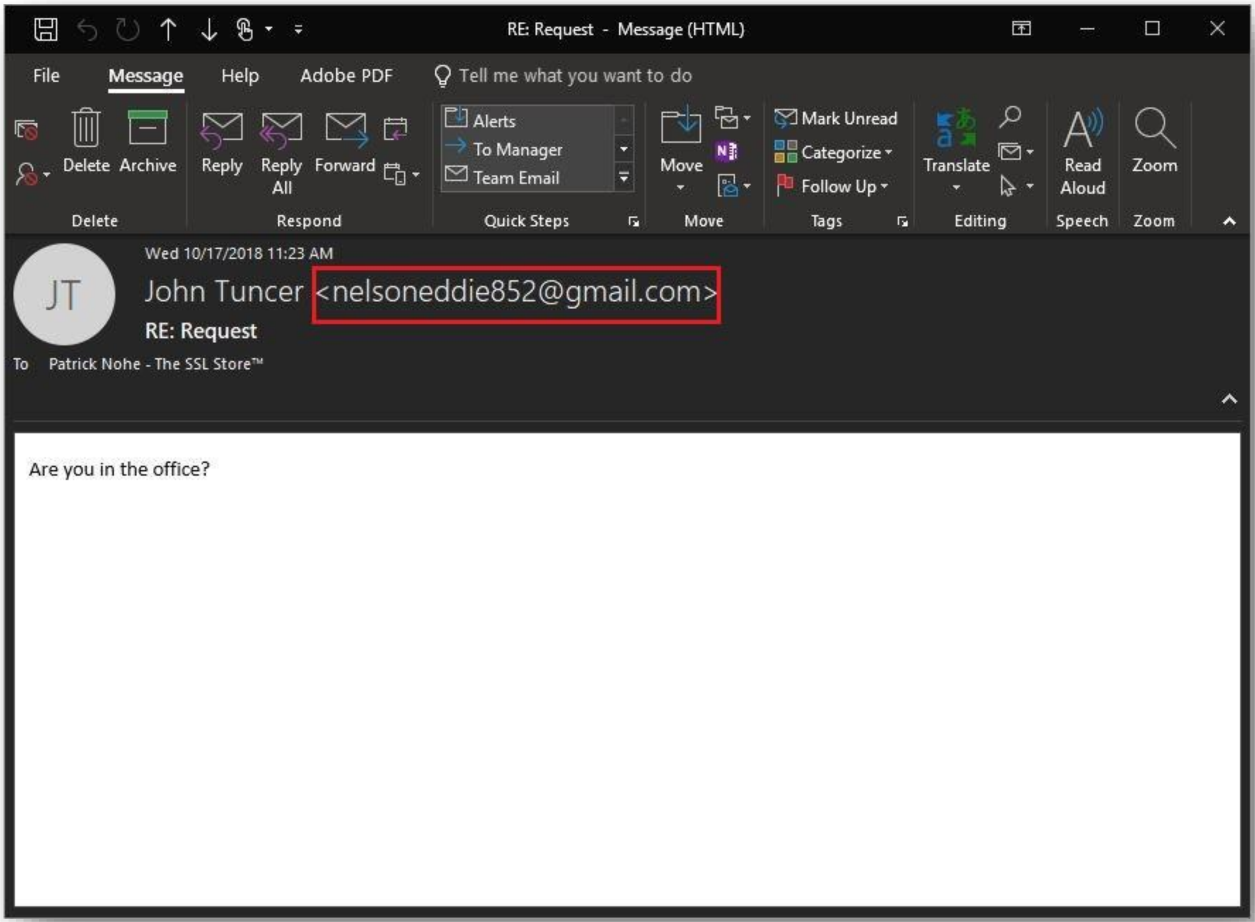


What your employees need to know

Staying high-level for a little longer, there are some general pieces of information that every employee needs to consider when trying to determine if an email is legitimate or phish. Let's run through them.

Learn how to determine the real sender

Obviously, the person or company that purportedly sent that email is not always who they claim to be. We've already discussed how to set up a number of mechanisms that prevent an attacker from imitating you, but when you're the one they're trying to dupe, not all of those things help. That's why it's absolutely critical that any employee should be able to identify the true sender of a piece of mail. And it's not the name that appears at the top of the email. Anyone can change that to anything they want. Teach your employees to search for the email address in the Header's "From:" field. Here's an example of a phish we received from someone impersonating our owner. Not only was it not signed, it's from a Gmail address.



Learn to use your S/MIME certificate

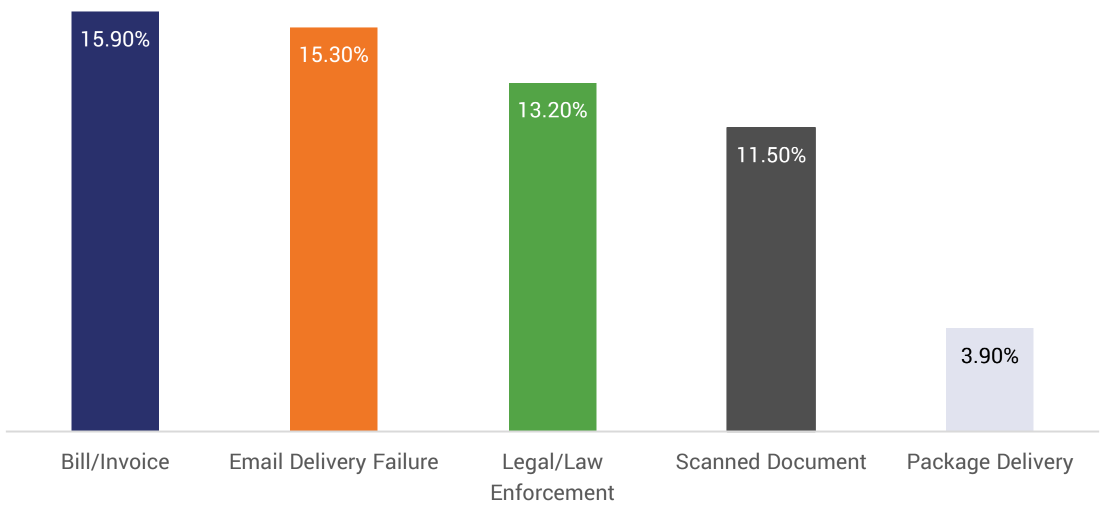
What good is an S/MIME certificate if your employees don't know how to leverage it? Your employees should know to do three very basic things once your organization begins using S/MIME.

1. Always check if an email is signed. If it comes from within the organization, it should always be signed.
2. Sign all outgoing email. If you aren't signing, the recipient will have a harder time verifying the email's legitimacy. This costs time, and by extension, money. Get into the habit of signing everything.
3. If an email is important, or contains sensitive information, encrypt it. Encryption will prevent anyone that's not authorized from reading it.

Don't ever panic, rush or buy into a perceived sense of urgency

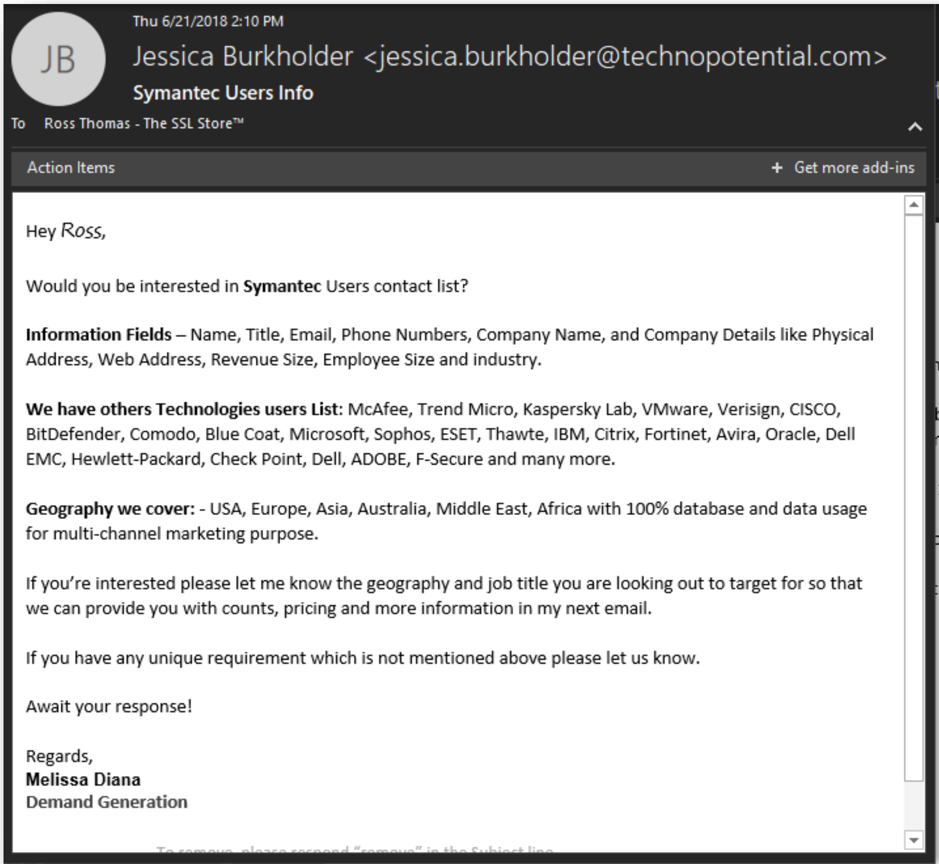
As we covered earlier, the best phish are designed to play on our emotions and impulses. Remember, the attacker is trying to trick you. And most people don't think clearly in a snap. That's exactly what these criminals are going for. So, if you receive an email with an aggressive subject line, or the email requests you take immediate action on something, stop, calm down and let your cooler head prevail. If this were really an emergency, the other party would be using something a little more urgent to get in touch with you, not email. Most email that requires some kind of urgent action is a scam.

Malicious Email Comes Disguised As...



Impersonal greetings are a dead giveaway

Almost categorically, if the sender of an email doesn't bother to use your name, meaning they instead opt for a very general greeting using a pronoun like "employee" or "customer," at best it's a mass emailed advertisement, more likely it's spam or phish. Most spam, and many phishing emails are generated using some sort of automated process. A template is written or generated, and sometimes a database full of names, email addresses, account IDs, etc. (typically stolen) is used to fill it in with information and send it out into the world. Let's look at a practical example:



JB

Thu 6/21/2018 2:10 PM

Jessica Burkholder <jessica.burkholder@technopotential.com>

Symantec Users Info

To Ross Thomas - The SSL Store™

Action Items

+ Get more add-ins

Hey *Ross*,

Would you be interested in **Symantec** Users contact list?

Information Fields – Name, Title, Email, Phone Numbers, Company Name, and Company Details like Physical Address, Web Address, Revenue Size, Employee Size and industry.

We have others Technologies users List: McAfee, Trend Micro, Kaspersky Lab, VMware, Verisign, CISCO, BitDefender, Comodo, Blue Coat, Microsoft, Sophos, ESET, Thawte, IBM, Citrix, Fortinet, Avira, Oracle, Dell EMC, Hewlett-Packard, Check Point, Dell, ADOBE, F-Secure and many more.

Geography we cover: - USA, Europe, Asia, Australia, Middle East, Africa with 100% database and data usage for multi-channel marketing purpose.

If you're interested please let me know the geography and job title you are looking out to target for so that we can provide you with counts, pricing and more information in my next email.

If you have any unique requirement which is not mentioned above please let us know.

Await your response!

Regards,
Melissa Diana
Demand Generation

Right off the bat, there are several things phishy about this email:

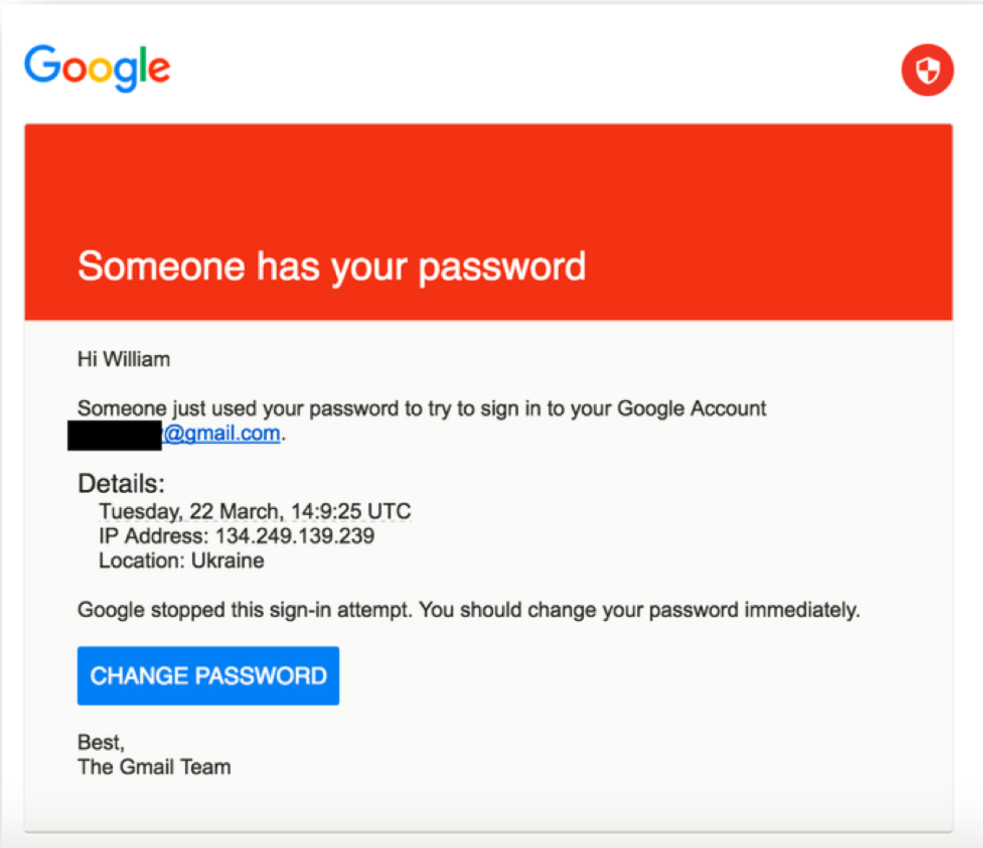
- ✔ The word 'Ross' is in a different font.
- ✔ The 'From' header, shows it's from Jessica Burkholder (Jessica.burkholder@technopotential) but that doesn't match the name in the signature, Melissa Diana.
- ✔ The content is shady (trying to sell a user contact list).

This email is spam, or possibly something more nefarious.

Don’t rely on images or logos

Unfortunately, it’s trivially easy to rip off a legitimate website’s logo, its email signatures, pretty much anything that is public facing. Because of that, you need to be careful not to get sucked in just because an email looks professional or authentic. You still need to do your due diligence before acting on it. As we discussed earlier, this most often takes the shape of brand phishing. An attacker will create an extremely convincing email template and use it to try to harvest credentials from unwitting internet users.

Here’s an email like the one that compromised John Podesta in 2016:



This looks like Google, it smells like Google. It’s not Google. It’s a phish. And unless you looked at the address of the sender, it would be easy to fall for. That leads us to…

Don’t click on links from unfamiliar senders

If someone you know sends you a link in an email that you think is legitimate, you should still hover over it with your mouse to see where it leads. But if you don’t know the sender or have even the vaguest suspicion that something might be amiss, don’t click it. Period. Full stop. Once you leave the confines of your inbox and follow a link out on to the web it might be too late. Don’t let it get that far. Teach your employees not to click on any links included in email from unknown senders.

16

The number of malicious emails the average employee receives per month

Don’t open attachments, either

Unless you can confirm its authenticity, never open email attachments. Organizationally, try to make use of a cloud sharing platform to eliminate the need for sending attachments entirely. While only one in 10 phish include malware, according to FireEye the average employee receives 16 malicious emails per month, with some industries, like Government/Public Administration, receiving over 50 per month. So, don’t get too hung up on the fact it’s just 10%, because given the volume of email sent and received daily, that 10% is still fairly significant.

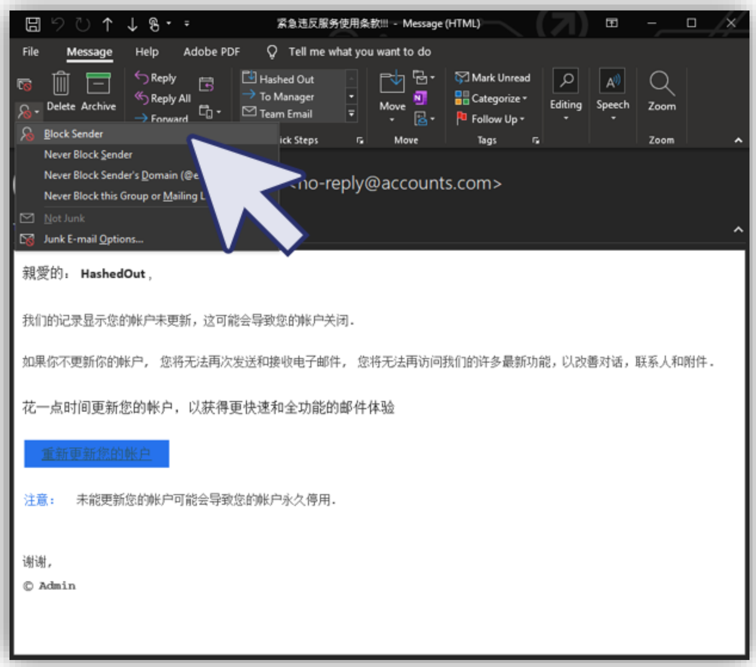
Rank	Industry	Emails per Employee
1	Public Administration	53.1
2	Wholesale Trade	34.4
3	Mining	30.0
4	Agriculture, Forestry & Fishing	26.5
5	Manufacturing	25.5
6	Non-classifiable Establishments	21.8
7	Retail Trade	19.9
8	Construction	18.1
9	Services	12.1
10	Finance, Insurance & Real Estate	9.1
11	Transportation & Public Utilities	8.7

Grammar Matters

One of the quickest ways to tell whether an email is legitimate or not is just to read its contents. Generally, in the business world, people try to write in coherent sentences that get spelling and grammar mostly correct. Very few of us are perfect when it comes to writing, but there's a difference between the occasional literary gaffe and a spam message written by someone who speaks English as a second language. If the email grammar and style doesn't sound like what you'd expect from the sender, flag it. Better safe than sorry.

See something, say something

Anytime you receive a suspicious email, flag it—tell someone. This will help keep your spam filter strong, plus, not reporting suspicious messages only increases the chances that someone else in your company gets phished. A good IT admin can create special rules to block certain IP addresses or domains from being able to reach your inbox. But they can't do that if they don't know.



When in doubt, pick up the phone

If you're ever uncertain whether an email was legitimately sent from the individual it's claiming to originate from, there's a simple solution. Call them. Seriously, just pick up the phone and dial their number/extension. They'll be able to tell you whether it was really them pretty quickly. And if they have no idea what you're talking about or why you called, that lets you know that you're going to need to speak with your IT guy because your company is being targeted. This should be your failsafe anytime you have a question about an email's legitimacy. Just call and ask.

Is this email for real? A cheat sheet

Here's a quick checklist that employees can use anytime a suspicious email arrives in their inbox – work or personal. Obviously, this is just an informal reference, it's not meant to supplant any educational materials or training that you may already be using.

#	Question	Yes	No
1	Is this email from someone you work with?	Question 2	Question 3
2	Is the email signed?	OK	Fail
3	Do you recognize the sender?	Question 4	Question 7
4	Does the sender match the address?	Question 5	Fail
5	Does the email pass the smell test? (Style, tone, signature)	Question 6	Fail
6	Is the email requesting something?	Call and confirm	OK
7	Does the email look official?	Question 8	Fail
8	Google the sender/organization, are they legitimate?	Question 9	Fail
9	Is the email requesting you take an action?	Call and confirm	OK

What we hashed out…

- 1 in every 101 emails is malicious and 97% of people can't spot a phish.
- Education is the best weapon against phishing. Phishing doesn't compromise technology, it compromises people.
- Sender Policy Framework tells an email's recipient if the domain it came from was authorized to send it.
- DomainKey Identified Mail uses a cryptographic signature to help determine if an email was truly sent from a given organization or domain.
- Domain-Based Message Authentication, Reporting and Conformance is a DNS-based protocol for dictating how an email's recipient should deal with SPF and DKIM failures, in addition to how they should be reported.
- S/MIME certificates add a much-needed layer of inner-organization security by asserting verified sender identity.

Call Us, We Can Help

How about a free consultation so we can discuss what your organization can do to secure its email against the threats of today? We work directly with our CA partners to offer the lowest prices in the industry. Email security for your entire organization is just a phone call away.

Phishing and email attacks in general aren't going to stop. They're a fact of life nowadays in the digital age. But that doesn't mean your organization can't defend itself. This eBook is the product of over a decade's worth of experience in the cybersecurity sector. We've been helping organizations secure their email since the day we started. As always, we're here to help. If you have any questions, we're standing by throughout the global workday. 24/7/365. Ask us how we can help you better secure your organization today.

The SSL Store™
146 Second St. N. #201
St. Petersburg, FL 330701
(727) 388-4240