Tis the Season to be Spammed!

Today we are going to talk about that dirty four-letter 'S' word: Spam. I won't lie, I hate this time of the year when it comes to providing email support. Spam, or spammers to be exact, are my arch nemesis. But today, we will be going over how spam works, what these spammers are doing, and why. I will also give you some tips and tricks to help you effectively manage your spam and provide some insights on what you can do in the future to avoid getting on some of these spam lists.

So why do I hate providing email support so much this time of the year? Because the number one question that I start to hear, and then hear many multiple times each day for the next 90 days is: "Why am I getting more spam?" It's like a Christmas song that you hear over and over. It's not that I hate answering the question. In fact, I love helping my customers, but it's simply that I have to repeat it over and over. There are so many moving parts, it takes a while to explain and sometimes gets lost in translation.

So, I'm fixing that this year. This article is meant to answer this age-old question one last time, which can then be shared many, many, many times. ☺ Please, please, feel free to share!

If you are under a time constraint, hate to read, or you just don't care why or how, you can skip all of this and go directly to the tips and tricks, but I think you will find this article to be very helpful and answer all of your questions!

No thanks, take me to the tips NOW.

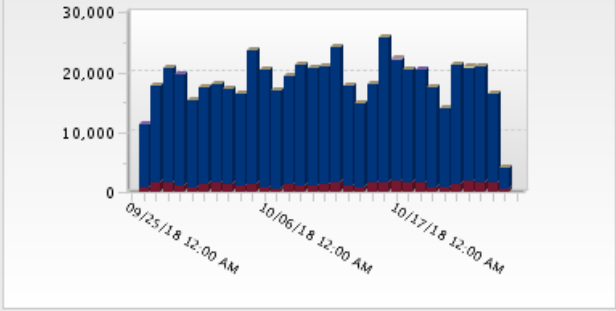
Why oh Why?

So why do we get spam and why do we get so much now, even before the holiday season starts? As with all things, it all comes down to money. Spammers use various tactics to collect your information, which is then sold to companies that use it to make a profit during the holiday season. Sure, these lists are sold throughout the year too, but the majority of money for these lists is made right before the holiday season starts. But spammers have to make sure their information is accurate before the holiday season hits. The more accurate the list is, the more it is worth when it is sold. Companies don't want to spend money on lists of users that no longer exist.

To get ahead of the holiday curve, spammers are most active in October.

At CDS, we have multiple email filtering servers to provide redundancy and to increase performance and delivery times. Below is a screenshot taken on 10/26/2018 of the activity across all of our email filtering servers representing the previous 30 days of filtering. Unfortunately, the software doesn't show us a larger range of time, but you can get a small glimpse of the growth pattern in the top chart. It is growing each week. If we were able to compare it with the previous 30 days, I can tell you that the average daily email flow was about 10,000 per day. The email total has grown by almost 30% in October and it will only grow each day until we peak sometime in early December. The charts can be a little confusing, because they report a mixture of both connections and messages. For all intents and purposes, each connection represents about one message. Therefore, we use them synonymously.

Messages	Count	%
Single threat messages:	577,123	78.1
Multiple threat messages:	102	< 0.1
Total Threat Messages:	**577,225**	**78.1**
Clean messages:	161,665	21.9
Total Messages:	**738,890**	**100**



Threats	Count	%
Content violations:	84	< 0.1
Malware:	140	< 0.1
Invalid recipients:	0	0.0
Bad reputation:	533,765	92.5
Spam and unwanted mail:	43,341	7.5
Disarmed Messages:	0	0.0
Threat Defense - Advanced threats:	0	0.0
Total Threats:	**577,330**	**100**

In these charts, each of the bars represent a single day. The days with the highest spikes are usually Mondays. The lower bars are for the weekend days. The screenshot was taken in the early morning, so the last bar represents the email received so far for that day. At a quick glance, I'm sure this snapshot in time doesn't mean much to the average user, but to a well-seasoned technician, it says a lot. It also helps to know the background and history of these reports, which is why we keep an eye on them on a weekly basis at a minimum. Large changes in email being processed, up or down, could lead us to identify a problem. When there is a problem, we occasionally make small filtering changes to further protect our customers, but we keep our changes to a minimum for the most part.

One of the statistics that we look at regularly is the total percentage of 'Clean messages'. This chart is showing that about 21.9% of all email being processed is considered clean and should be delivered. On average, the range for clean messages is normally between 11% and 13% throughout the other months of the year. For the percentage of clean messages to be this high, we know that a significant volume of spam is making its way through the filters. That number could be as high as 16,000 additional emails being allowed to go through in this 30-day time period. Something that we have to factor back into the equation is that the volume of legitimate email also increases considerably during the holiday season. However, we know the volume of legitimate holiday season email typically doesn't pick up until about the end of the first week of November.

Another interesting thing to note in this snapshot is the total volume of 'Bad reputation' email shown in the bottom chart. This large number represents the servers on the internet that try to connect to our filtering servers. This number is normally much lower. Closer to about 200,000 or 250,000 at most. As you can see, this is a little over double of what it would normally be. Bad reputation is similar to ignoring an incoming phone call using the 'caller ID' feature on your telephone. When an email server on the internet tries to connect, the email filtering server handling the request looks up that server's IP address or name in a special database of non-compliant servers. If the sending server is on that list, then our servers simply ignore the connection. This drastically reduces the amount of email that has to be filtered and processed, because the email is never transmitted. Out of the 577,000 total connections made to these servers, 533,000 were blocked! Our filtering servers have software that accesses a database of the bad servers and updates every 15 minutes to current. Although

the software is installed on our servers and maintained by CDS, this database is managed and maintained by the software manufacturer and is one of the major benefits of the monthly subscription that we pay for.

These lists are over 99.99% accurate.

The 'Spam and unwanted email' section of this snapshot is the last thing we need to cover in this report. This volume is showing us about 43,000 emails were accepted by this filtering server from email servers on the internet, but the content violated a spam policy and it was quarantined. This means the email is being held and won't be delivered. This volume is also about 30% higher than normal, which allows us to more accurately determine how many spam emails are really coming through. This would give us roughly 13,000 more spam messages that made it through for this 30-day period.

And one last thing about the quarantine. These are emails that are about 99.99% guaranteed spam. Sure, it can be wrong on occasion, but since they are in quarantine, they can be released for delivery. We don't review the quarantine, because the volume is just absurd and our server filtering pricing doesn't take that time into account. So, in the rare case that you haven't received something you are expecting, simply give us a call and we can look it up for you.

Let's go 'phishing'

With people changing jobs or internet providers, millions of email addresses are created or changed daily.

This is why spammers can never stop working to perfect their lists.

To improve the accuracy of those lists, they are constantly testing your email accounts throughout the year. Spammers build distribution lists of valid email addresses and prune any email addresses that are no longer valid. The most basic tactic used to test the validity of an email address is a concept known as 'phishing' or 'email phishing'.

Email phishing is easy, cheap, and very effective. Throughout any calendar year, spammers send occasional emails to each email address in their lists to see if they are still valid. If the test email bounces back, they know to remove it from their list, otherwise they have confirmed that the email address is most likely still in use. It's like casting a line out into the sea or pond. If you get a bite, then you know the fish are out there, otherwise, you can take that spot off your list and move on to a new fishing spot. This common analogy is why it is called 'phishing'. But why use 'ph' instead of just an 'f'? In the mid 90's, hackers that were using these tactics were called 'phreaks'. Instead of using an 'f', they substituted 'ph' in the name, which lead to the replacement in the phrase email phishing.

Flying under the radar

Spammers use many different tactics to bypass or circumvent spam filtering systems. One of these tactics I call the 'drip effect'. It's like a faucet in your home. You aren't as likely to worry too much about a faucet that drips every once in a while. It has very little effect on your water bill, and like many of the projects around my home, it seems like more of a nuisance to fix than it would be to just let it go for a while. Yes honey, I'll get to that this weekend.

If a spammer sends a test email to your account once per month or even once per week at the most, you aren't as likely to do something about it. Neither is your email provider or filtering service. If their users aren't complaining, then there's no reason to take the time to work on locking down the filters. This allows spammers to build their lists with new email addresses and make their existing lists more accurate without causing too much suspicion.

Another important factor with flying under the radar is where and whom the spam is coming from. It would be too easy to block a single spam server or email sender, so spammers often hijack legitimate email servers or email accounts to send out spam. This makes it much more difficult to differentiate spam from legitimate email.

What can you do to stop spam?

You can't. Period. Sorry, I know that isn't the answer you were looking for and I know it's painful to hear, but there are things we can do to reduce the amount of junk email (spam) that you get. But why can't we stop spam? The answer to that question has enough content for its own article and then some. Maybe that is something I will do in the future, but it is out of the scope of this article. In a nutshell, it's like junk mail that you get from the post office. You have a valid address; therefore, junk mail can be sent there.

Yes, we have email filters in place and yes, we have opt-out lists that are mandated by laws to keep spammers in compliance, but enforcing them is a different story altogether.

Simply put, if the spammer exists outside of the country, it's nearly impossible to enforce. Even if they are within your borders, the costs to do so are often too high to make it worthwhile.

It's much more cost effective to click the delete button than to call your lawyer, or worse yet, attempt to contact the government.

And to circumvent the opt-out rules, a spammer only has to create a new organization or email address to send from each time they send out email. It's like in the old days when we used to block incoming calls to our home and then receive the same type of call coming from a different phone number.

False positives – it's not you, it's them

Those email filters… why can't we just block all spam? Email filters are a collection of complex algorithms and business logic. I could give a week-long seminar on how spam filters work and why they will never catch everything. Spam filtering gets better every day, but then again, so do the spammers. They are constantly working on testing new tactics to get those emails through.

Keep in mind that spammers and hackers are constantly developing new techniques to trick or bypass email filters. This is why we buy email filtering software that updates itself with new virus and spam definitions every 15 minutes. The annual or monthly subscription to those software manufacturers pays for them to improve and catch these new spamming tactics as they are discovered. This is also why you will see some spam flood through, only to resolve itself a few days or weeks later.

This is why spam will never go away completely.

Ultimately, this time of year, you are bound to lose some of your email to spam filtering software that is in-place somewhere. Some of this may be under your control, but most of it isn't. If you control the filtering software that your company subscribes to, then you may be able to fiddle with it to make it more accurate. But beware, it's very time consuming and even easier to make a mistake and block legitimate email.

I'm here to tell you, it is stressful and it is something you will probably give up on after a few short weeks. The time commitment itself just isn't worth it compared to paying a filtering company like ours to do the work for you. You need to ask yourself, is it REALLY that hard to delete an email you don't want so you can avoid sacrificing the delivery of one that is important?

Each year, we are ready for the calls: "I sent an email to a customer and they didn't receive it." Most of the time, it isn't you, it's them. Around this time each year, the big players in the email game are getting call after call about the increased levels of spam coming through. Companies like Verizon, Comcast, Yahoo, Microsoft, and even AOL (yes, I said AOL), start getting aggressive and begin locking down their email filters. Inevitably, they all go too far. Their changes start blocking legitimate email. We call these false positives, because it falsely identified a legitimate email as a spam message. And if you wanted to know… Verizon is the biggest culprit for the past three years running. It's nice that they want to be proactive, but they tend to make the most mistakes when doing so. Sorry Verizon.

As a hosting and filtering company, we have a much smaller footprint than the other big names, therefore we are usually not as much of a target for hacking or spammers. While there are some benefits of going with a bigger hosting or filtering company, we don't get as much spam as they do. This is a big differentiation between our email hosting and filtering services and those of the big players in the game that I previously mentioned. It is not necessary for us to continuously try to lock down our filters. Our filters are mostly 'out of the box' configured. They do such a great job, that we don't need spend a lot of time changing them. This means that our false positives are much, much lower than our big competitors. I'm sorry, I would much rather have you get an important email and have a few extra spam messages to delete than to miss a big sale or worse, a customer complaint that goes unchecked. Trust me, a few extra pieces of spam aren't a big deal. Let me explain why…

You don't know how good you really have it

Face it people, we are spoiled. The spam filters in place today are a thousand times more effective than they were 30 years ago. I remember back when most of the people I knew didn't even have an email address, and I still received over 200 emails per day and probably 95% or more of them were spam. In just the past decade, we have reduced the amount of spam received by about 80% or more. Most spam filters will accurately filter out about 90%-95% or more of all spam. The concession is that we, of course, don't want to lose any legitimate email, so casually hitting the delete button for spam email is almost always the best alternative to missing something important.

Let's take this information and put it into perspective though. You saw how big the numbers were for the filtering service for all of our filtering servers. They have processed almost 3/4 of a million email messages in a 30-day period. We represent well over 2,000 email accounts that we provide filtering services for, but we will only use 2,000 in our calculations. If you take the total number of increased spam messages (~13,000) that we identified earlier and divide that by the low range of email accounts (2,000), that gives us an increase of about 6.5 additional spam messages being received per person every 30 days. That's only 2 extra emails per week! What?! Yep, it's a small, small figure. Remember, I said we are spoiled? And I'm no exception to that rule. I just have a lot of years of experience in my field, and I feel privileged to know the inner workings of email filters to know that I should bite my tongue when I get those nasty 'S' letter word messages.

I know, I know… You get more than 2 extra emails per week. Remember, our math just averaged those new spam emails over all of the accounts. Some of us who have had an email address for a really long time, or those of us who are very active online, will most likely get the bulk of those new emails. The other, luckier users will probably see almost no increase in spam.

You are your own worst enemy

In this decade, and specifically within the last 3-5 years, the majority of email we get that we consider spam is actually legitimate email. We easily lose sight of the many emails we are bombarded with throughout the day that we have to manage. Facebook, LinkedIn, Best Buy, fast food restaurants, and many other retail stores are constantly sending us email to stay in front of us. Suggestive selling is a great way to improve sales. If you get that restaurant coupon email at just the right time before lunch, you might end up going there. (Yes, I'm guilty too.)

The problem is that you are inundated with so many legitimate emails, that when you have to deal with those few spam emails, they end up being the straw that breaks the camel's back. Those emails become more noticeable, even though the increase of those emails is so few in the grand scheme of things. There are many things we can do to help fix or reduce this problem. I have included some of these great ideas in the tips section at the end of this article.

Tips & Tricks for reducing spam!

Fixing the problem, not the symptom

Often, we try to solve symptoms instead of the real problem or root cause. Imagine you are late for work. That may seem like a problem, and it most likely is if you ask your boss, but that isn't really 'the problem'. That is a symptom of something else. Maybe you ran into traffic because there was an accident or you got a flat tire. And yes, I'm being positive and didn't mention the fact that you stayed up all night binge watching your favorite TV show and slept through your alarm. Your tardiness is a symptom of the real problem. The real problem is what we call 'the root cause'.

The amount of spam you receive is often the symptom, not the original problem.

With spam, the root cause most likely occurred weeks, months, or even years ago when you signed up for a free toaster or entered for a drawing to win a free vacation. We hate to be left out. We all want a chance to win something. These are just a few tactics that spammers use to get your contact information. If you willingly enter your contact information into an entry form, they have permission to use it however they want to. Most of the promotions or prize drawings are scams that are only used to collect your email address, phone number, or mailing address. Don't expect to win anything any time soon. And if you do, I would be even more cautious. Some of those prizes you think you are winning are just scams to get access to your computer or other confidential information. If the promotion or prize drawing isn't offered directly through the original vendor's website, then it's probably a bad idea to give them your information.

The 12 ways you can reduce spam are…

1. Don't sign-up for promotions or enter into online drawings

   Everyone wants to be a winner or get something for cheap, but your sanity and possibly your identity is on the line every time that you do. The more someone knows about you, the easier it is for them to gain access to your financial information or steal your identity. Heed the age-old saying that if it is too good to be true, then it probably is. Before you fill out that online form, just ask yourself, 'am I willing to clean up more spam every day or even lose my identity over a $50 gift card and a chance to win a free computer'. If you want more information on how this works, you should read the main content of this article above to know why you really aren't doing yourself justice when you sign up to win things on a website.

   And respect the privacy of others. Most of these online gimmicks and promotions ask you to enter at least one other email address of a family member or friend for better chances to win or for a chance for them to also win. Trust me, you aren't doing them any favors. You are only exposing their email address and ultimately causing them to receive more spam too.

   Keep in mind that large retail or chain stores will respect your privacy, so entering into a drawing or signing up for a promotion on that company's website is typically safe and pretty common. They don't want a PR nightmare of legal battles over not obeying compliancy rules. But just keep in mind that you will start to become inundated with a lot of email. Legitimate companies will allow you to opt-out of those email lists, but as part of the fine print when you sign up, you may be allowing them to share your contact information with their suppliers, vendors, or other third-parties. They often receive money for this information. This could be a long laundry list of companies that you have never done business with. As part of the compliance rules, you would be required to opt-out of each service separately to stop receiving those annoying emails coming from those third-parties.

   As a general rule of thumb though, only enter for promotions or prize drawings from well-known companies. They are less likely to sell your information and more likely to obey any

guidelines or compliance regulations to avoid bad publicity. And if you aren't sure, read the fine print. What you find yourself agreeing to may be alarming.

2. Only sign-up for companies that you want to hear from regularly (a lot)

If Starbucks, McDonald's, or a retail store is one of your regular hot spots, then there is nothing wrong with signing up for promotions or coupon alerts. It could save you a lot of money in the long-run by being able to take advantage of their many coupons and offerings. But just remember, we have to clean up those emails too. They don't disappear on their own. On average, I'm willing to bet most retailers send at least one email per day, and that often doubles or triples during the holiday season. It adds up fast. Imagine being subscribed to just 5-10 lists. That could mean cleaning up as many as 70+ additional emails per week! But we have a few nice tricks to help you manage that. Keep reading…

3. Download and install the app instead

If you still want coupons for those restaurants and retail stores, most of them have an app you can download for your phone and/or computer. Most vendors require that you create an account to use their app. This automatically signs you up for their email lists. After you sign up and create an account, you can go back in to your account and opt-out of the daily emails. This allows you continue to use the coupons and promotions found in the app, but removes the abundance of emails that you get every day. You may miss some specials, because not all vendors mirror the promotions in-app and through the emails, but most do. If you have to have both, then read the next trick.

4. Hide that legitimate spam

I consider 'legitimate spam' regular emails that you receive from email lists that you want to be part of. If you like receiving daily emails for various restaurants, retail stores, and other subscriptions, but you don't want to micro-manage them and delete them individually, then here is a nice trick for you.

Most email applications, like Microsoft Outlook, have the ability to create email rules. A rule tells the system what to do with an email based on the sender, subject, content, attachments, or even who the email is addressed to. While there are many other types of rules, the most common are rules based on the sender (who the email is coming from). When your email application receives an email from that 'sender', it performs an action that you specify on that email. The two most common actions people use are 'delete' and 'move to a folder'. Here's how I use these email rules to control my inbox and keep that legitimate spam down to a manageable level.

First, I create a new folder called 'Promotions'. You can create a folder with any name of your choosing, but I give it this name, because it helps differentiate legitimate email from real junk mail or spam. I don't want to accidently mark a legitimate email as spam. I then create rules for each vendor that move all incoming email from those vendors into that new folder. This does a few important things. First, it very quickly and automatically separates important email from the not-so-important email. My inbox is cleaner and it helps me avoid missing important emails among the many slew of coupons and promotional material that comes in daily. Second, it saves me a lot of time from managing those emails. Since most of those types of emails are time sensitive, I know that I can normally delete them after 30 or 60 days at most. And because they are all in one folder, I can quickly select all emails older than a certain number of days of my choosing and delete them, which only takes about 1 minute to do. I can do this manually once per month or I can set up an archive rule that does it automatically.

The nice thing about this is that you don't have to do this all at once, and I wouldn't recommend investing all of that time anyway. When an email comes in for a specific vendor, I take that opportunity to set up that rule. In my version of

Microsoft Outlook, I simply right-click on the email message, select 'Rules' from the menu and then select the option 'Always Move Messages From: [sender's name here]'. I can then select the 'Promotions' folder. It not only moves that new message, it also goes through all of the existing messages in your inbox from that sender and moves those too!

One thing to note, sometimes vendors change the email address they are sending from, or they have multiple email addresses that they send from based on product, service, or promotion. Sometimes, your rules will become outdated and need to be updated with the new sender address. This is as simple as deleting the old rule and creating a new one.

This is my absolute favorite trick, because I get the best of both worlds. I continue to get the coupons and promotions, but they are on my terms. And better yet, it doesn't make a mess of my inbox. If I feel like going to a restaurant and need a coupon, I simply go to this folder to find them. I organize by date and all of the newer emails are at the top.

Bottom line… It's a game changer. If you don't know how to set up email rules, call CDS for assistance on setting up email rules to clean up your inbox.

5. Unsubscribe

Be careful when you unsubscribe (opt-out) from an email list. If you are opting out of a well-known company, then they will most likely abide by the rules and leave you alone. Keep in mind that you may continue to receive emails for a short period after unsubscribing because some systems take a week or so to update your removal request. However, if it is a company you have never heard from, don't know who they are, or it just feels shady, don't try to unsubscribe. We explained earlier in this article a trick called 'phishing' that spammers use to verify your email address. Another trick spammers use to verify your email address is opt-out trickery. They provide you with an opt-out link in the spam email, but when you get to their opt-out page, they want you to enter your email address. You may be tempted to oblige when they ask you to enter email addresses of your family and friends, but this is a bad idea. Entering your email address in the opt-out page does two things: confirms that your email address is valid and if you enter more than one email address, it validates those email addresses too. You might think you are doing your friend, family member, or coworker a favor by entering their email address, but you are probably doing the exact opposite.

The general rule of thumb is to only unsubscribe from well-known vendors. If you get a small amount of other spam emails, then manually delete them. If a particular vendor sends many emails, and the 'from' address never changes, then set up a delete rule to take care of those. For the pros and cons of using delete rules, please see below.

6. Set up delete rules or mark as spam

Keep in mind that not all companies are unethical. They are simply trying to market their products and services like the well-known companies do. There will be times when you have a company that isn't well-known, but they send you a lot of email. No, it won't kill you to take the chance of trying to unsubscribe from their mailing list. That choice/risk is yours, however, there are other alternatives.

As explained earlier with hiding legitimate spam, we can set up rules to process incoming email. We can use these same rules to move or delete email that comes in from a specific sender. You can apply these same types of rules to delete these emails or to move them to the spam folder. If you are deleting them, I would suggest creating a delete rule. If you are moving them to the spam folder, then I would use the spam mechanism within your email program. This will keep your email rules list much smaller and logically place the spam rules where they should be: in the spam list.

The one thing you need to be aware of is that most spammers change the sender's address every time they send an email. In this case, you are not likely to get an email from the same sender again. Since delete rules and marking items as spam are based on the sender, you are just wasting time creating a rule or marking it as spam. I manually delete most of my spam, but I keep an eye on any patterns from a specific vendor or sender. If the sender doesn't change, then I know a rule or marking it as spam will work. Otherwise, I suck it up and just hit the delete button.

7. Subscribe to a good filtering service

There are many email filtering services on the market to choose from, and of course each has its own pros and cons. Choosing a good filtering company can be as much about luck as it is making an educated guess based on fact and online articles or reviews. I relate choosing providers for services like this to Goldilocks and the Three Bears. Some service providers are just too big. While they usually have very strong resilient networks to minimize downtime, these larger companies are often targets for more spam and hacking. This causes them to be more reactive and make a lot more changes to their filters, which can ultimately cause issues. On the other hand, a very small company can provide a more personalized service, but they usually lack the network resilience. They will be less of a target, but you may experience a lot more downtime than you would like. The best compromise is a company that has a more solid foundation than a small startup, but doesn't have the global presence of a large company. This will often provide a better experience all around. I'd like to think our company, Computer Development Systems, is one of these providers.

When doing your research, don't get too hung up on the features being provided by each of the providers. They are often just fluff and if the past dictates the future, you will never use them beyond the first few times you try them. The more features that a provider implements, the more issues that can occur and the more they have to support. There are really only a few important features that you need look for.

1. The most important, of course, is the success of the filtering engine. If you see a lot of complaints about missing important email, then walk away. This means they are trying too hard to perfect the impossible. In fact, you want to find a company that is mostly hands off from the software they are using. The more they dabble, the more problems they create. Remember, most filtering software is 99.99% (or more) accurate, so there shouldn't be much there for them to do.
2. Make sure they have a quarantine. A quarantine is where spam or potentially bad email is stored before it is deleted permanently. This allows the filtering company to release a valid email that might have been filtered, which is considered a false positive. This means that you can contact the provider and ask if there is anything in quarantine from a specific person or domain.
3. Make sure they have some type of reporting system that you can look up email activity or they can do it for you on your behalf. While this is very helpful to find email that was caught by the filter, this has been invaluable in troubleshooting email issues or helping resolve customer/vendor discrepancies over the past 20+ years. I'm not sure how many times a customer has called asking for a delivery report for an invoice they sent to a customer that claims they never received it. Just keep in mind that most vendors usually only store the last 30 days of history due to the sheer volume of email that they process.

8. Buy your own domain name (it's cheap!)

If you use a free email account through a large vendor, like Verizon, Comcast, Microsoft, Yahoo, AOL, etc., you have very little control over the spam filters and how they work. You can't use a third-party to provide email filtering, so you are

required to use their filtering services. Sometimes, you are also stuck with keeping their internet services, because you don't want to lose your email address. For example, if you have Verizon internet at home and instead want to take advantage of a Comcast internet deal, you have two options: switch your email address to a new Comcast address or pay Verizon a monthly fee to keep your email address. Ultimately, you are inconvenienced each time you switch email providers or you forfeit some of those savings when you have to pay a monthly fee to keep your email address. Free isn't always free long-term.

By purchasing your own domain name, you can then choose your own email hosting company to host your email and provide email filtering services. It allows you to control your email addresses, hosting, AND filtering services. This also means that it doesn't matter which internet provider you choose or switch to, because you are no longer locked in to their domain name or email services. This also drastically reduces your spam, because all of your email addresses are new and spammers won't know they exist.

'Registering' your own domain name is cheap. People say 'buy', but they really mean 'rent'. You pay for your domain name annually. When you stop paying, you lose it, so you never really 'own' it. If anything, you 'own' exclusive rights to use it. A domain name of your choosing is purchased from a registrar and can range in price depending on which registrar you purchase from, the number of years purchased, and the domain extension (.com, .us., .net, .org, etc.) chosen. Registering a domain name is easy, but managing it and configuring settings can be overwhelming for most. You need to be on top of things to make sure your domain doesn't expire and you lose it to someone waiting in the wings for you to forget to renew. At CDS, we offer a domain renewal service to avoid those mistakes. We monitor the renewal dates of the domains that we manage and notify our customers 2-3 months before they expire. We register, configure, and monitor the domains on your behalf.

After you purchase a domain name, all you have is a name reservation. You need to choose a hosting company to provide an email server to host your new domain name and receive email. This is similar to a PO box at the post office. It is a physical location on the internet where everyone sends email that is designated for you. The hosting company receives and sends email for you and the servers are available on the internet 24/7 so you don't miss any incoming email. Hosting pricing varies widely and choosing a hosting company can be daunting, but you often get what you pay for. Average pricing is about $15-$20 per month, but please contact us to go over options and what to look for when choosing a hosting company.

9. Change your email address (it's easier than you think)

The most effective way of reducing your spam is to change your email address. If you create a new email address, it's like starting over when it comes to spammers. They have no idea you exist. You have essentially changed your email identity. You are like a stealthy email ninja, and from this point forward, you can use all of the previous rules to reduce your spam long-term.

It's easy to create a new email address. Either follow tip #8 and get your own domain name or just create a new email address with your existing provider. You could simply add or remove a letter or number from your email address, or go with something completely different, that is your prerogative. Regardless, the result is the same… less spam!

The trick to changing your email address is in the execution. After you create (and test) your new email account, you will do two things: set up a forward from your old email address to your new email address and you will send all future emails out AS the new email address. The email forward will guarantee that you don't miss any email while

you make the transition. You will continue to keep the old email address in place for about 1 year or whenever you feel that you have migrated everyone over. When you notice that none of the email coming in addressed to the old email address is legitimate, you may turn off the email forward and get rid of the old email address and all of the ugly spam that came with it.

What you will NOT do is create an auto reply in your old email account that notifies everyone of the email address change.

All this does is alert the spammers that your email address has changed and defeat the purpose of creating the new email address!

All new emails that you send should be sent from the new email address. You should no longer send email out using the old email address, because it just sends mixed signals to your audience. Sending out email using only your new email address allows users to easily reply to your emails and add the new email address to their address book, as well as get your contacts in the habit of using your new email address. You may want to put a message in your email signature line indicating that you have changed your email address and that they should update their records, because not everyone notices a change. See below about why you should add it to your email signature instead of sending out a broadcast message with your new email address.

10. Properly send out broadcast emails

When you create an email with a large number of contacts in the 'To', 'Carbon Copy (CC)', or 'Blind Carbon Copy (BCC)' fields, it is considered sending a broadcast email. This is considered passé and is frowned upon. There are a few reasons why you shouldn't send out emails this way.

A lot of spam filters will block emails coming through with too many email addresses in the email. Combining many email addresses into one spam message is a very old tactic used by spammers. Believe it or not, this also opens you up to more spam. If someone you know sends out a broadcast email with your email address in the CC or To field, and any one of those people addressed in that email gets a virus or malware, your email address is exposed. If they would have sent that email to each person individually, then your email address would not have been exposed to someone else's virus. While you can't control what other people do with your email address, you can help guide them on what they should or shouldn't do when you see it happen.

It is also considered rude to send broadcast emails. You are sharing people's email addresses with people they probably don't know. It can make some people feel uncomfortable that you are sharing their email address with others. The recommended way is to send an email to each person individually, when possible.

Broadcast emails do, however, have their place in some instances. There may be times that you want or need to send an email to a group of people on the same topic and you want each person to be able to respond to all members and see other responses from the group. This is the true intention of a broadcast list. If you need each person to be actively involved in the conversation, then you should limit the number of recipients to less than 10, if possible. The lower the number of recipients the higher the success rate for delivery.

11. Stop clicking on those links and images

When you receive spam or unwanted emails, you may be tempted to click on the 'unsubscribe' links or images found in the content of the email. Unless the email is from a well-known company, it is highly recommended that you don't click on any links in these emails. The links often have codes in them that help identify your email address. When you click on those links or images, that code is transmitted to the sender's server. The server receives that code, pairs it up with the email address it was sent to, and then marks that

email address as valid. Essentially, you just verified your email address for them.

You should also beware when clicking on links or images in an email, because it could open your browser and download a virus or malware. The most common trick used by spammers and hackers is to provide you with an email that scares you into a call-to-action. They ask you for login names, passwords, or account information. Some of those examples are:

- Your package is being held and will not be delivered unless you click here and authorize its release.
- Your invoice is overdue and it is attached. Please pay or you will be sent to collections.
- Your taxes are overdue and you must click here to pay them or you will go to jail.
- Payroll is delayed, click here to verify your account information.

I'm paraphrasing, but I think you can get the point. They play on your emotions, mainly fear, to get you to open something or enter your login name and password into a bogus website. These are just tactics to steal your information.

12. Don't let images come through

Another trick spammers use is sending tracking images in their emails. The emails contain mostly images with very little content. Don't let them fool you with a catchy subject line to get you to download the images. When you download the images to view them, they can have an embedded code that validates that you received the email. You don't even have to click on the image, just view it.

Most email programs, like Microsoft Outlook, block images from being displayed in the emails that you receive until you allow them to come through or request to download them. This may seem annoying, but it solves a few problems. Because the images are not downloaded until you want to see them, it makes the email content load faster and saves bandwidth for the sender of the email. Their servers aren't being hit all at once to provide that image. It spreads it out over a longer period of time and is only provided to each user as they view the email, which ultimately provides a better user experience. However, more importantly, as mentioned above, it avoids those images automatically being downloaded and verifying your email address!

So, as a general rule of thumb, only download images for emails that you really want or need to see the content for. If you trust the sender, then you can often select an option that will always download images from that sender to avoid that extra step when working with that sender.

A final word

Don't let spam get to you. Reducing the amount of spam you receive is similar to taking care of your health. It's not a sprint, it's a marathon. You can't do just one thing to lose weight or to get in shape, and it won't happen overnight. Reducing spam takes awareness of your actions and long-term commitment to the cause. But I assure you, it is worth it in the end. Hopefully you can utilize some of these tips to greatly reduce your spam stress, allowing you to live a longer and happier digital life.

Coming Soon: ITDirt.com

We will soon be providing you with relevant IT information, or 'the dirt'.

We want to share our ideas, tips & tricks, item sales, and general IT information with our customers and the world. We are working on a new website ITDirt.com to do just that. We will be providing blogs, newsletters, and webcasts to share in 2019 and beyond. Please watch for the website to unfold and new information to come…

We look forward to an exciting 2019!