Doing IT Right
What Happened to My Email?
By Barry Mishkind

[June 2019] For most of us, email is still a vital method of communication and information sharing. However, over the years, email has become problematic in a number of ways, from spam to "missing" emails. What are useful solutions?

Email is not what is used to be.

When I opened my email this morning, there were about 30 messages that were clearly spam sitting in my system. And that is only what got through the filters.

Why are there so many spams? I have used my main email address for over 25 years. It was simple and worked well.

Of course, back then there were no dictionary attacks – where each name was tried on every domain possible. Nor were the lists scammers share of "good" addresses very large. (You may also wish to review Steve Tuzeneu's article on how your address could be on a spam list.)

Worse, some emails I expected were "missing" for all intents and purposes.

What is going wrong with email today?

ONCE UPON A TIME

There was a time, when you sent an email and it was received almost simultaneously.

Everyone agreed that was a major improvement from the old Bulletin Board System (BBS), where messages took a day or two to circulate.

However, it did not take long for spammers (one of the first was said to be an attorney) to scrape addresses off the "newsgroups" and other places that brought people together on the Internet. Today, estimates are that some 70 – 90% of all emails are spam.

EARLY PROTECTION

It is unlikely you will find anyone who likes spam – whether it comes from the prince in Nigeria or the company selling lotions to increase the size of your private parts.

But, that dislike has created its own set of problems that have resulted in your email not reaching its destination and/or replies not get to you.

Today, spammers have acquired nearly 8 billion (yes, billion) email addresses – shared among the bad guys. So users and the ISP industry react by creating spam applications to automatically block or trash unwanted email – as well as your wanted emails.

PROGRESSIVE IDIOCY

Perhaps you have seen the character named Mordoc in the comic strip *Dilbert*.

One basic idea around the character is that he is the head of Information Prevention – among his tricks is preventing email delivery. That way, there can be no spam.

That may sound ridiculous to you, but hold on a moment. *Dilbert* can be spot on.

These days many companies institute every possible protocol, from blocking IP addresses, issuing "challenge" responses, greylisting, to whitelisting – likely one of Mordoc's favorites.

A few years ago a major radio consolidator IT department once instituted a whitelist – without informing staff. That included emails from ad agencies not in the approved whitelist! One can only wonder how many buys were lost.

THERE MUST BE A JOKE HERE

I know for a fact that this is true because at one time I was casually trying to make arrangements for lunch with a friend. But, he never responded;

Finally, I picked up the phone and asked why he had not responded to my invite. He said he never got any such email – despite ten or more tries. A bit later, he called back, explaining IT had put a whitelist in place without his knowledge, and he was missing a lot of emails.

At least I can report that once management understood what was going on, the whitelist disappeared.

But, as the song goes, there is more.

PROTECTION GETS OUT OF HAND

Many of us maintain and use several different addresses – for work, one for personal use, or other reasons. Some do work better than others, but each has potential benefits and traps.

As as example, as email servers have consolidated email jas become much more fragile than it ever was – with many emails seeming to just "disappear" into the ether.

Starting with AOL and Yahoo, there was strong use of DKIM and DMARC tags. They and other email providers started sending emails where the "From:" and "Sender" fields differed into a digital trash bucket.

Mordoc would be pleased.

MORE FILTERS, MORE OFTEN

In addition, many ISPs put into place other filters that dump emails into spam folders – of you can find them. And then, false positives make can cause a new set of problems.

Unfortunately, all it takes is one bad actor on your node (did you know cable systems have as many as 1,000 users on a node?) to add your address to a "Realtime Blackhole List" (RBL).

I found this out when I could not send email to a friend on the *very same cable provider.*

After climbing several levels of supervisors, I got one in Atlanta to admit there was little they would do because, apparently, another person in my neighborhood had been reported as a spammer and was entered into an RBL. All I could do was wait it out or use another ISP.

THE LAND OF LOST EMAIL

And, yes, it can get worse.

If you use an email address different from your cable Internet address, it is possible some poorly thought out servers, like the barracuda, will block your email because the IP address does not match the email domain.

A major hassle happens when someone decides to unsubscribe from an Internet mailing list by marking a message as spam instead of taking the time to unsub properly. Users Yahoo or AOL, for example, can find all messages blocked from a list due to someone marking that list as spam in order to unsubscribe.

Another problem is when a spammer spoofs *your* email address in the "From:" field. Often what follows are emails and phone calls from hundreds of people "yelling" at you to "stop the spam."

The result can even make conducting business impossible for a week or two.

FALSE POSITIVES

Did I mention false positives?

My original address, perhaps the one many of you know, has been in use for 25 years. Spammers are the reason I now let it go through Gmail for filtering.

Even then I regularly have to retrieve missing emails for that address. Even if I have marked them as "not spam" Gmail often continues to put emails from the same sender into the spam folder. Annoyingly, there is no support/service from Google to try to fix things.

So, are there ways to overcome these problems or is email essentially headed for extinction?

SO WHAT CAN WE DO?

It would be wonderful if there were something easy like a tracking number for email.

True, one can do a traceroute or use other approaches to find where email goes off the rails, it is very time-consuming and not very easy to successfully find the bad link or filter – and the reason. That is, of course, the way the hackers like it – they can hide in the darker places of the Internet.

A more productive approach actually might be to call the person with whom you want to communicate. The trouble is, phone spamming is now so bad that if the other guy does not recognize your number, he may not pick up at all – a good reason to ensure your outbound caller-ID is working.

In many cases, regularly examining any spam folder you or your ISP uses is important. Marking something as "not spam" may or may not help. Adding your friends' email addresses to your address book works in many cases – especially if you both do it.

WEB INTERFACES

It is generally true that using a web interface for most ISPs will get usually get your email out,

On one hand, such web interfaces usually can be more reliable at sending emails by stripping out your local IP address, to avoid IP based filters. On the other, it is not as convenient as using your own mail reader.

Some web interfaces (i.e. Gmail) even let you use your "primary" email address to send from their system. If you find your primary address blocked, this is a good way to overcome it.

THE ULTIMATE

If you browse the websites of various companyies, it can be hard to find an email address aside from a generic info@company.com address.

Instead, you often find yourself looking at a web email form. You can enter your message and send it – right after you respond successfully to the captcha box to prove you are not a robot.

The one downside is that you rarely can get a copy of your message for your records, unless you remember to copy and paste.

SO WHAT ELSE CAN WE DO?

If you are starting a new email account, consider using either first initial and last name and/or a number of some sort. As noted, it will reduce spam filter positives.

If you have a lot of critical email, perhaps involving money and/or contracts, consider using an ISP with real customer support that will actively help block spam while working to ensure your emails will be delivered.

On your end, it is probably useful to check what filters are in use. Sometimes you might find it is your own outlook.com account that is blocking emails.

JUST DO NOT ASSUME

Well, you know the phrase.

The idea is that if some important email seems to be missing, take the time to investigate.

Over time, it will make your email more reliable. Still, we can expect more changes in email usage as various entities struggle to find better ways to fix things and thwart Mordoc. - **BDR**

- - -

Do you enjoy articles like this about new gear?
Sign up (it only takes 30 seconds) here for the one-time-a-week BDR Newsletter.

- - -

Return to The BDR Menu