THE EMAIL HAS LANDED:

HOW UNDERSTANDING AND IMPROVING DELIVERABILITY CAN HELP YOUR MESSAGES GET THROUGH

JANUARY 2018

SoftVu

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Email marketing turns 40 years old in 2018.

When Digital Equipment Corporation's Gary Thuerk[1] sent a unsolicited sales pitch to 397 Arpanet users on May 3, 1978, a new type of selling was born.

And so was spam.

Thuerk's stunt annoyed many of his recipients. It crashed some systems. Thuerk was reprimanded and told not to do it again. Still, his pitch led to millions in computer equipment sales.[2]

Four decades later, email remains the top vessel for business communication. In 2017, 3.7 billion worldwide email accounts sent an estimated 269 billion emails every day.[3] That's a lot of inboxes -- and a lot of messages competing for attention.

Yet one in five emails won't land in an inbox at all[4] , getting bounced or detoured into a spam folder instead. Even the sharpest message won't generate a single sale if the intended recipient never sees it.

Understanding deliverability -- getting your message where it needs to go -- is essential for today's marketers.

[1] Julia De Simone, "*Meet the 'Father of Spam', a Goodyear Resident,*" Arizona Republic, March 31, 2016. Web.
[2] Kate Stoodly, "*Father of Spam Speaks Out on His Legacy,*" eSecurity Planet.com, November 19, 2004. Web.
[3] "*Email Market 2017-2021,*" The Radicati Group, June 2017. Executive Summary
[4] "*We Know Email: Secrets of Best In Class Email Senders*", Return Path, April 2017

And it's a job that must start long before you write a single word.

Deliverability means being precise.

It means being strategic.

It means building and protecting a virtual reputation.

And it means adhering to an always-evolving code of conduct that largely remains a secret. The entities who make and enforce the rules won't tell the public exactly what these rules are.

There are, however, practices widely believed to boost the odds that your message will hit its target. Those who know how to play the game can have the vast majority of their emails avoid the spam folder and land in the inbox.

We're about to share advice that may help.

THE REVOLUTION AND EVOLUTION OF EMAIL

To understand how email works today, you need to know how it began.

Email as we know it dates back to 1971[5], but it spent its first 20 years primarily used by scientists, universities and computer buffs. As the internet became user-friendly in the early 1990s, dial-up service providers like Compuserve and America Online began including email service in their subscription packages. Still, email was mostly a tool for business and early adopters. The average person didn't have an address.

In 1996, Hotmail changed the game by offering free web-based email accounts to anyone who wanted one. Within six months, a million people had signed up.[6] Yahoo! began offering its own free email service the following year.

Marketers now had a fast, inexpensive way to reach mass audiences and they took advantage of it. Respected financial, travel, restaurant and retail giants discovered email was a good way to contact customers. Users also saw their inboxes flooded with unsolicited offers -- some of which had viruses and porn.

Scammers discovered email, too. "Phishers" sent mail purporting to come from a recipient's bank in the hope they'd reply with personal information. Non-existent Nigerian princes promised vast riches in exchange for quick cash.[7] Both ruses worked.

[5] "1971: First network email sent by Ray Tomlinson," ComputingHistory.org.uk. Web.
[6] "P.S. I Love You and Get Your Free Email at Hotmail," Techcrunch.com, Oct. 18, 2009. Web.
[7] Katherine Trendacosta, "Here's the best Nigerian prince scam in the galaxy," Gizmodo.com, Feb. 12, 2016, Web

A nonprofit called the Mail Abuse Prevention System (MAPS) began tracking junk emails, now frequently called "spam" after a memorably annoying Monty Python sketch.[8] MAPS gave subscribing network managers a "Real-Time Blackhole List" of senders and spam-friendly domains to block.

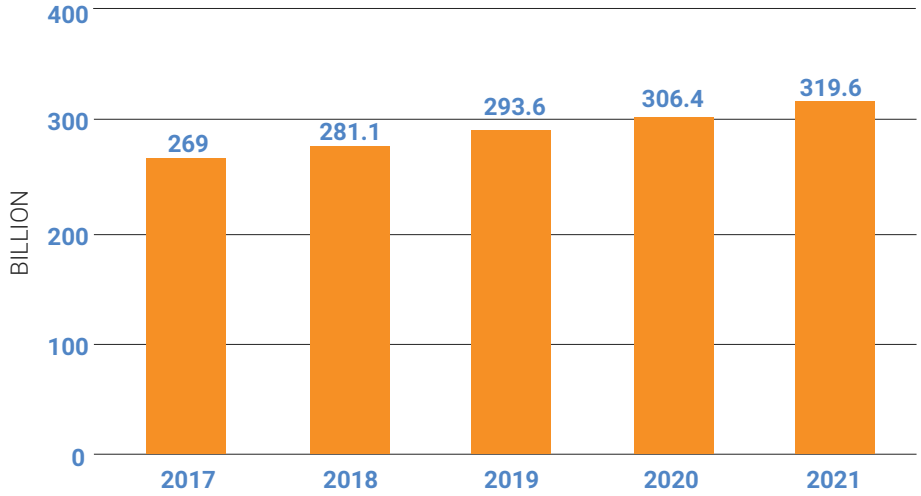
Before long, major mailbox providers were letting users mark unwanted messages as spam and exile them to a special folder.

Still, a lot of nuisance, fraudulent and porn-filled emails got through the system -- and the flood was only starting.

Spam expert Steve Atkins warned the Internet Engineering Task Force's Anti-Spam Research Group (ASRG) in 2003 that spam volume was growing by 20% every single month. He predicted that without massive spam-blocking improvements, users would eventually be getting 140,000 pieces of spam *every day*.[9]

The public demanded stronger action. The federal government finally responded.

PROJECTED WORLDWIDE DAILY EMAILS



SOURCE: RADICATI GROUP

[8] Justin Gmoser, "Monty Python is the reason we call junk email spam," BusinessInsider.com, Jan. 27, 2017. Web
[9] Anti-Spam Research Group Meeting Report, www.ietf.org, March 20, 2003. Web.

CAN-SPAM

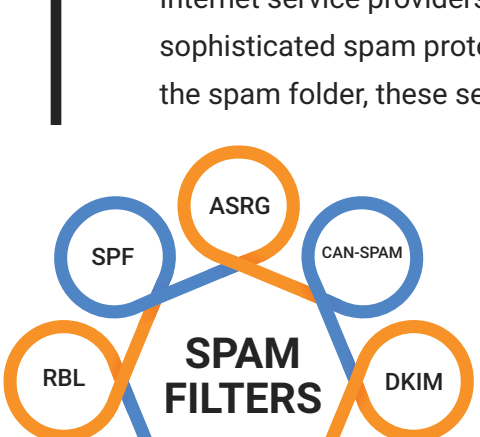
In 2003, the first national commercial email standards arrived in the form of the Controlling the Assault of Non-Solicited Pornography and Marketing Act. CAN-SPAM, as it was called, required all commercial email messages to include:[10]

- Accurate sender information and subject lines
- Disclosures identifying an ad as an ad
- A physical postal address
- A way for recipients to opt out of future emails

While these rules were welcome, they were not aggressively enforced.[11] CAN-SPAM also drew criticism for nullifying more stringent state laws, including regulations requiring marketers to label ads in the subject line.[12]

"The entire Act should be thrown out and replaced. It hasn't worked to control spam, and it has, in fact, only served to make the problem worse," anti-spam crusader Ron Guilmette said.[13]

Internet service providers tried to differentiate themselves by offering more sophisticated spam protection. Instead of letting recipients exile unwanted mail to the spam folder, these services began letting their algorithms sort it for them.



ASRG - Anti-Spam Research Group
CAN-SPAM - Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
DKIM - DomainKeys Identified Mail
DMARC - Domain-based Message Authentication, Reporting and Conformance
ISP - Internet Service Providers
MAPS - Mail Abuse Prevention System
RBL - Real-Time Blacklist
SPF - Sender Policy Framework

*** See Glossary of Terms on page 21**

[10] CAN-SPAM Act: A Compliance Guide for Business, FTC.gov
[11] "With This Law, You Can Spam," WIRED, Jan. 23, 2004
[12] Christopher Brown and Lesley Fair, "Candid Answers to CAN-SPAM Questions," FTC.gov, Aug. 18, 2015. Web
[13] Brian Krebs, "Is It Time to Can the CAN-SPAM Act?" Krebs On Security.com, July 2017. Web

THE ALL-POWERFUL PROVIDERS

Gmail, Yahoo!, the various MSN domains and AOL now dominate the mailbox operation business. Their algorithms give them the power of police, judge and jury over what constitutes spam, and this authority makes them significant gatekeepers.

Gmail alone has more than a billion monthly users.[14] If Google's filters determine a sender's messages are spam, it can block that sender from many or even all of Gmail's inboxes.

These companies also know how their users engage with each email they get. Are they opened? Are images activated? Do they click on links? Do they add the sender to their address books? Or do they delete the email unread -- or worse, mark it as spam?

Each factor adds data to the formula providers use to set their filters. But they largely keep the data -- and their formulas -- a secret. These mailbox providers *could* decide to post clear rules for what will get an email marked as spam. They just don't.

They also tweak those formulas all the time, without telling anyone how or even *if* it changed. This leaves marketers like a pitcher throwing high heat at an arbitrary strike zone. And senders often didn't know their messages were being treated as spam.

These filters can ensnare many legitimate emails. As email grew, so did demand for new ways to help protect legitimate senders and recipients. This need gave rise to three validation mechanisms: SPF, DKIM and DMARC.

[14] Frederic Lardinois, "Gmail now has more than 1B monthly active users," Techcrunch.com, Feb. 1, 2016

THREE MECHANISMS FOR ENTRY

Emails have to pass the transparency test before they can enter the inbox. Each one has to basically state who they are and on whose behalf they are being sent. Over time, three mechanisms have been created to help reduce the amount of unwanted emails – SPF, DKIM and DMARC.

SPF

Spammers sometimes try to bypass filters by making it appear the email is coming from a trustworthy source, a practice known as "spoofing." To fight this, Sender Permitted From -- later renamed Sender Policy Framework -- was created to help block mail from forged addresses.[15]

With SPF, a domain owner creates a list of anyone authorized to send emails on the domain's behalf. The receiving system cross-checks the sending server's IP address with the sending domain's list. If there isn't a match, the receiving system may block the email or send it to a spam folder.

SPF is similar to a nightclub doorman checking a list of approved guests before letting a customer in. What it **doesn't** do is check the guest's ID to verify that he or she is who they say.

Because it's older and easier to use, SPF is fairly common. Domains that don't use it have a much higher risk of having their emails blocked.[16] But because it does nothing to verify a sender's identity, DKIM arrived in 2005 to add an extra layer of protection.

DKIM

DomainKeys Identified Mail, a marriage of mechanisms initially designed by Yahoo! and Cisco[17], verifies emails are from legitimate sources and haven't been changed in transit.

[15] "Sender Police Framework: Introduction," OpenSPF.org, April 17, 2010. Web.
[16] Brittany McCluster, "What are DMARK, DKIM and SPF?", Inbox Pros.com, June 15, 2017
[17] "DKIM Frequently Asked Questions," DKIM.org. Web.

A sender using DKIM signs outgoing emails with a private "key." The recipient can check this signature with one published on the sender's Domain Name System. If the keys match and the content was unaltered, the recipient's system can let the email through. The sender's domain has vouched for the email's authenticity.[18]

With DKIM, think of having a pizza delivered. When the driver, "Joe," is at your door with the pie, you call the pizza shop and ask if Joe is the guy they sent. If they confirm it and the box is still sealed, your pizza is probably OK to eat. Dig in!

DMARC

A third mechanism, Domain-based Message Authentication, Reporting and Conformance (DMARC), arrived in 2012 with the backing of top providers and financial industry giants. It combines elements of SPF and DKIM and adds even more features.

DMARC is the first of the authentication mechanisms that can ensure that the name in the "sender" line -- the one the recipient sees to determine where an email comes from -- is accurate.[19] In other words, the email is from who it says it's from.

The recipient can also set up policies outlining what to do with emails that fail SPF or DKIM tests. This policy can be strict and bounce everything, it can move emails to spam folders or it can send it on through. The recipient may also choose to report back to the sender whether that message passed or failed.[20]

Think back to the DKIM pizza delivery. Say the shop tells you they don't have a driver named Joe. But this stranger at your door has a hot, tasty pizza -- and you're hungry. Maybe you're tempted to take a chance. DMARC lets users set firm rules to save them from their worst impulses.

[18] DKIM.org. Web
[19] Matt Moorehead, "*How to Explain DMARC in Plain English,*" Return Path.com, July 20, 2015
[20] "*Frequently Asked Questions*". DMARC.org. Web

DMARC offers the most protection, but it's also the most complicated -- and least used -- of the three. In March 2017, the Federal Trade Commission surveyed 569 businesses and found only a third of them were using DMARC. Less than 10 percent use DMARC's strongest setting to block unauthenticated messages.[21]

THE BOTTOM LINE

With multiple systems in use to catch spam and bounce suspicious emails, marketers must be precise in how they set up their mailings -- and then test, test, test.

Small errors in SPF or DKIM code can not only get one email blocked or sent to a spam folder, it can create a ripple effect on future mailings. Recovering from this ripple effect can become a costly, drawn-out process.

You don't want to go to the time and expense of acquiring leads, only to have your messages never reach them. Everything needs to be in great shape in order to have the best deliverability experience. You also want to make sure your online reputation is as good as it can be.

[21] "Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication," FTC.gov, March 2017

PROTECT YOUR REPUTATION

Every internet service provider and every IP address has an online reputation in regard to email, depending on its record of results. This reputation matters. A good one is like a high credit score[22] -- you're seen as less of a risk and people will be open to doing business with you.

Some mailbox services -- not all -- will give you basic information about your reputation. Third-party companies also offer to assess a user's reputation with report cards, using either a numeric or a positive-neutral-negative scale.[23] Just as with that credit rating, it's a good idea to have a sense of where your reputation stands. Sudden changes can be a sign of trouble.

Some practices are reputation-builders. Using SPF, DKIM and DMARC verification with **error-free coding** will help. It's also a plus when recipients engage with your messages -- opening them, activating images or clicking links. If recipients add you to their address books, that helps even more.

Likewise, bad interactions hurt. If a large percentage of your emails go unopened or deleted, it indicates the recipient just isn't that into you. If it happens often enough, a mailbox provider may bounce your message back.

If a recipient goes a step further and marks your email as spam, you'll probably wind up in his or her spam folder next time. If they ask to unsubscribe, you'd better act fast to grant the request. Otherwise, future emails to them will also be unwanted, may be marked as spam, and could ding your reputation every time.

[22] "*We Know Email: Secrets of Best In Class Email Senders*", Return Path, April 2017
[23] Jillian Wohlfarth, "*5 Ways to Check Your Sending Reputation,*" Sendgrid.com, March 9, 2015

Error-free verification coding aside, many of these reputation factors depend on how recipients react. The best you can do is earn their trust, craft appealing messages and hope they engage. But some of the most damaging things you can do to your reputation are *entirely* in your hands.

If you're using a new IP address -- don't start by sending a tsunami of emails right away. Warm it up with smaller, targeted mailings so you can form a good reputation and let it build. This will help you more with spam filters than being an unknown commodity.

Once you've been mailing for a while, try to keep your volume consistent.[24] Someone who's been steadily emailing 5,000 customers may raise a red flag if that number makes a sudden spike to 100,000. Pace yourself -- or the filters may doubt that all of your thousands of new leads are legitimate.

Even if you've had a "positive" reputation for years, a sudden change to a sales-y message or subject line can cause a batch deliverability issue, making it difficult to regain your previous squeaky-clean reputation. Knowing how to adjust, or better yet, plan ahead by to "pulling the levers" behind the scenes can go a long way to remain in good graces. It's never easy to crawl out of a hole.

SPAM TRAPS

Some email addresses floating around the web have been put there for the sole purpose of luring spammers. These "trap" addresses aren't associated with any real people and you don't want to get caught using them.

"If you're sending emails to spam traps, it's considered an indicator that you've used bad practices to collect email addresses -- or at the very least, you didn't do a good job of keeping your list clean," said Bettina Specht.[25]

[24] "*We Know Email: Secrets of Best In Class Email Senders*", Return Path, April 2017, p.5, Ebook
[25] Bettina Specht, "A Guide to Spam Traps and How to Avoid Them," Litmus.com, April 18, 2016, Web.

There are all kinds of spam traps. "Pristine traps" are never-used addresses that are floated into online communities as bait for people compiling and selling giant email lists. Sending emails to these addresses will likely ding your reputation.

Other trap addresses are recycled from long-inactive email accounts or dead domains. If you're emailing someone who hasn't logged in for a decade, the two of you probably don't have a solid business relationship.

Some trap addresses are created with deliberate typos -- @gnail.com, for example --- in hopes of ensnaring bulk marketers using automatic address generators. Because customers can make typos -- or use fake addresses -- when they sign up, the consequences for these traps aren't as tough as the others.

You're more likely to find bait addresses in mass quantities of unvetted leads.[26] Keeping clean mailing lists of people who indicate they want to hear from you can help you avoid spam traps. Conversely, sending email blasts to every address you can come up with is inviting trouble .

The good news is that the better your reputation, the more likely an infrequent error will be seen as an honest mistake. Good online citizens whose emails typically reach and engage legitimate customers will find forgiveness far faster than junk marketers who bend or ignore the rules.

THE BOTTOM LINE

Email campaigns come with a reward and a risk. It's an inexpensive way to reach a lot of people at once, but if they don't welcome your message or they mark it as spam, it can hurt your future marketing efforts.

[26] "A Brief Guide to Spam Traps," Wordtothewise.com, August 5, 2011. Web.

It may be tempting to aim for quantity in the belief that a 2% return on 100,000 emails is equal to a 20% return on 10,000 emails, but it's not that simple. While each strategy may lead to 2,000 responses, a vast majority of the bulk messages may go unopened or get marked as spam. Sending 100,000 emails could prove costly to your reputation.

Choose your leads wisely and work hard to keep them engaged, a process that requires senders to be united, disciplined and strategic.

SMART STRATEGIES

It's critical for marketing teams and clients to work together to develop campaigns and solve problems when they occur. That means focusing on long-term strategies and reputation-building. A trustworthy brand will have more long-term success than a reckless huckster.

QUALITY > QUANTITY

In email marketing, precision messages to targeted leads will do more for your sales and reputation more than an email blast to every address in the country.

Think of two high school students looking for prom dates. One creates a clever, appropriate prom-posal that's perfectly crafted for the person he wants to ask. The other barrels down the hall, offering to take the first person who says yes. Both strategies may or may not pay off in dates, but the second student will surely leave some classmates thinking he's desperate -- and creepy.

Timing is also key. Be strategic. Because having recipients engage with your emails helps your reputation, don't send them when they're unlikely to be opened. Late at night -- or Christmas Day -- may be a bad time to pitch new services to banks.

It's also not a good idea to flood your recipient's inboxes. Sending one generic email in the morning and a similar-looking one a few hours later increases the chances that one -- or both -- will go unopened. Some annoyed users may even mark them as spam. Sending more than one message in a 24 hour period is risky. The recipient needs time to respond to the first email before getting hit with a second.

So in some cases, the best email strategy is not sending one -- and that's OK!

YOUR WORDS MATTER

"Look at me! I am spam!"

That's what some emails essentially say in their subject lines. You know what these look like. You've probably seen them a lot. They're so tacky that they almost dare you not to report them.

A message header written in all caps or with a lot of dollars signs and exclamation points often trigger spam filters. So can many common words and phrases, including "Discount," "Make Money," "Pre-Approved" and "Sale."[27] Even "this isn't spam" written in the subject line of an email will likely encourage filters to junk it. If your email looks like spam, it probably is.

FOLLOW THE LEADS

Email leads are like fresh fruit. If washed and well-inspected, they can leave you fortified, refreshed and energized. But if you just pick up and eat whatever you find laying on the ground, you may wind up feeling queasy and wishing you hadn't.

Vetted leads where you know the target has an interest -- and perhaps even the means -- to buy will serve you better over time than blasting messages to a million random people.

While lead sellers may dangle tempting offers for big batches of email addresses, you need to consider where those leads came from. Are these real people who have a legitimate interest in your business -- or were the addresses scraped from online forums or old mailing lists from long-defunct companies?[28]

[27] Karen Rubin, "The Ultimate List of Email Spam Trigger Words," Blog.Hubspot.Com, January 11, 2012. Web.
[28] "Where Spam Traps Come From and How They Work," Blog.Mailchimp.com, June 25, 2013. Web.

In a best-case scenario, a large chunk of those bulk lead emails may go unopened. Some users may mark them as spam. And this assumes you haven't stumbled into any spam traps. Enormous, poorly vetted email lists can be riddled with them.[29]

OPT-OUT AND FEEDBACK LOOPS

Listen to your customers, especially if they say they don't want to hear from you anymore. CAN-SPAM laws require emails to have a way to opt out of future mailings.[30] Not honoring that request in a timely manner can damage your online reputation. It won't do any favors for the image of your overall brand, either.

Some major mailbox providers, including Yahoo! and Hotmail, use tools called feedback loops[31] to let senders know when a recipient makes a spam complaint. The implicit message of the notifications are, "They don't want your email. Now leave them alone."

It's a good idea to be aggressive in monitoring and fielding these complaints, possibly using a dedicated email address to collect them. You'll be able to scratch those addresses off your send list right away -- before the next mailing goes out.

"Repeatedly sending messages to recipients who have opted out of those messages is the fastest way to tank your reputation," wrote Greg Kraios and Chris Arrendale.[32]

Tracking these messages -- which also show the header and body of the email that triggered the complaint[33] -- is also a good way to assess whether your message strikes users as overly spammy.

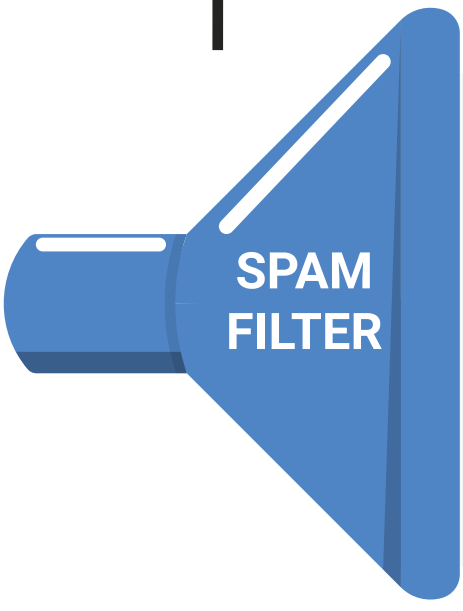
[29] Justin McHenry, "It's a Trap! Avoiding and Removing Spam Traps," Blog.Returnpath.com, March 11, 2016. Web.
[30] Christopher Brown and Lesley Fair, "Candid Answers to CAN-SPAM Questions," FTC.gov, Aug. 18, 2015. Web.
[31] Henry Gutierrez, "What is a Feedback Loop?" Blog.returnpath.com, March 29, 2017. Web.
[32] Greg Kraios & Chris Arrendale, "9 Things Every Marketer Must Know About Email," 250ok.com, Nov. 1, 2016
[33] Greg Kraios & Chris Arrendale, "9 Things Every Marketer Must Know About Email," 250ok.com, Nov. 1, 2016

BE ENGAGING

When you have people who do want to hear from you, make your messages worth their time. Write subject lines for your emails that make them want to open and read it. Once they're in, have an appealing pitch that entices them to download images, click links and maybe even reply.

For receptive prospects, employ a "journey" method that makes them aware of a need, gives them options to solve it and guides them toward the best solution.[34]

This means following well-received emails with additional messages that approach their problems from different angles. As long as recipients remain engaged, keep sending more fresh, interesting and perhaps personalized emails. Use any feedback you get to lead these users down a path to a sale.



Some words or phrases that may trigger spam filters [35]

- $$$
- Bargain
- Be Your Own Boss
- Bonus
- Buy
- Click Here
- Compare Rates
- Discount
- Earn Money
- Eliminate Debt
- Fast Cash
- Full refund
- Guarantee
- Limited Time
- Make Money
- Money Back
- Money-Making Opportunity
- Mortgage
- No Obligation
- Please Read
- Risk-Free
- Satisfaction Guaranteed
- Save $
- Urgent

[34] Lauren Hintz, "What is the Buyer's Journey," Hubspot.com, June 15, 2016, Web.
[35] Karen Rubin, "The Ultimate List of Email Spam Trigger Words," Blog.Hubspot.Com, January 11, 2012. Web.

CONCLUSION

Email marketing remains a powerful tool, but there's nothing worth less than a sales pitch that never reaches its target.

Systems are in place to keep unwanted emails out of user inboxes. Unless you understand and follow good practices, you run the risk of languishing in spam folders instead of in front of your potential customer's eyes.

Protect your reputation by targeting and nurturing legitimate leads. Write eye-catching subject lines that don't get ensnared in spam filters. If you use SPF, DKIM or DMARC -- and you should -- make sure your coding is error-free. And know that sometimes the best email strategy is waiting for the right time to send.

SoftVu will work with clients on smart strategies to stay in front of potential issues. With the right infrastructure, teamwork and a careful eye for detail SoftVu can make all the difference for your business.

GLOSSARY

ASRG - Anti-Spam Research Group - An international organization founded to study ways to protect email users from spam. It concluded its work in 2013.

CAN-SPAM - The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, the first national commercial email standards.

DKIM - DomainKeys Identified Mail - One of three major email verification mechanisms.

DMARC - Domain-based Message Authentication, Reporting and Conformance - The newest of the three major email verificiation mechanisms.

ISP - Internet Service Providers.

MAPS - Mail Abuse Prevention System - A nonprofit organization that started tracking spammers and spam-friendly domains.

RBL - Real-Time Blacklist - A frequently updated list of spammers and spam-friendly domains that MAPS shared with subscribers.

SPF - Sender Policy Framework -one of three major email verification mechanisms.

ABOUT SOFTVU

SoftVu, founded in 1999 and based in Kansas City, accelerates your sales conversion rates by creating, managing, distributing and tracking direct-to-consumer marketing campaigns. Leveraging big data, machine-learning algorithms and marketing automation, we deliver repeatable and predictable results to our clients, optimizing lead management strategies. For more information about SoftVu, visit www.SoftVu.com.

2029 Wyandotte St. Suite 100
Kansas City, MO 64108
(816) 895-8828
Toll free: 855-726-5763
info@softvu.com | softvu.com