

The Death of Email Tracking



Why are we writing this report?

Tracking a marketing email's open and click performance is something that every seller to schools does. But while some marketers tend to treat these stats purely as validation of a particular subject line or an insight into the performance of a particular CTA, others use them to make huge strategic decisions or trigger automated email sequences and workflows.

And it's for these businesses that we decided it was time to write this whitepaper.

Is Email Tracking Dead?

Well, no, it's not dead. But it's certainly sick, and probably terminally so.

Over the past five years we – like the rest of the email marketing industry – have watched as a new breed of email security software has steadily grown in prominence. This new breed of software works by interacting with your emails, usually by caching images or verifying the destination of URLs, in order to check the sender's authenticity or protect the identity or location of the recipient. These interactions then register as opens and clicks on your email tracking.



Does this mean my emails are being flagged as spam?

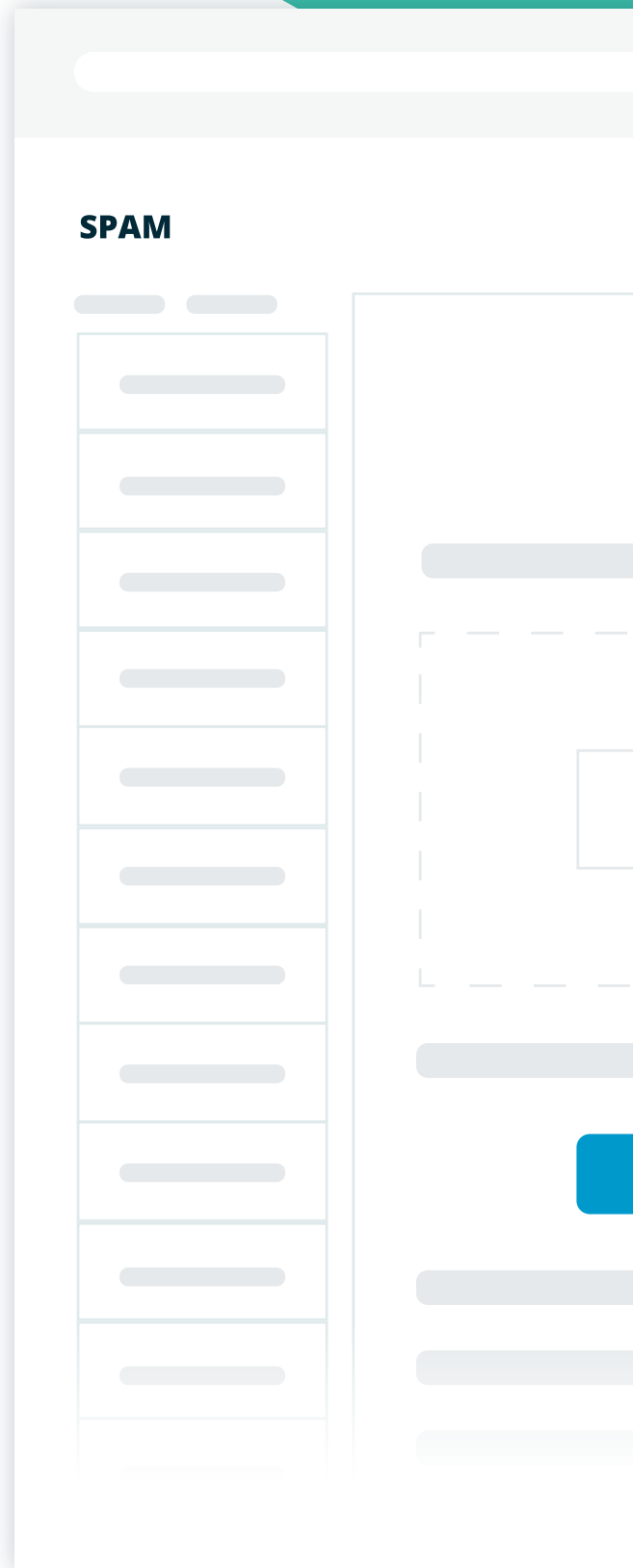
No.

It's important to say right off the bat that just because this email security software is interacting with your emails in this way, that does not mean that your email is more likely to end up in junk or spam folders.

It also doesn't mean that some of the opens and clicks you're seeing registered against teachers whose schools are using this software are not genuine. They may very well have opened and clicked on your email, the point is that it will be impossible – or nearly impossible – to differentiate between the genuine and the automated engagements.

What are the different software and scenarios at play?

Let's look at a chronology of these issues and provide an overview of how they impact – or will impact – your education marketing:



1. Email Clients Set to Automatically Download Images

How long has this been happening? 10+ Years

How Prevalent is this issue? Very High

How hard is it to spot? Impossible

When a marketing email is broadcast through any bulk emailing platform (Campus, MailChimp, HubSpot etc.) a tiny transparent image is inserted into your HTML – it can be as small as a 1 by 1 pixel – and when a recipient loads the images in your email this beacon image is downloaded.

What we're really measuring therefore, when we're tracking email opens, is how many times that beacon image has been downloaded.

Some email clients default so images are not automatically downloaded when a person opens an email. This is most common in Outlook and will mean that a teacher might open your email and read it, but unless they choose to download the images, you won't be able to track that they've opened it. It's estimated that between 17-34% of email recipients will open your email but not download the images and so cannot be tracked.

Conversely, some email clients will default to downloading images whenever a user clicks the email, even if it's just to remove the "unread" status or to view in a preview pane. Likewise, images will be downloaded if a recipient has an out of office auto-responder set up. In all these instances an "open" will be recorded, even though, in reality, the recipient may not have opened your email.

This issue has been at play for over 10 years but has become much more prevalent in recent years with the growth of teachers' viewing their emails on mobile devices (close to 70% of teachers have been opening email on mobile devices in the past 12 months, up from around 30% five years ago). On mobile, Apple and Google are the most common email clients and they usually default to automatically downloading images. While on desktop, Outlook is still the most common email client and usually defaults to blocking them.

All of this means that some teachers who register as an open on your email tracking will not have actually opened your email, while some teachers that did open and read your email will not register as an open.



2. Email Security Software Checking URLs in your Email

How long has this been happening? 5+ Years

How Prevalent is this issue? High

How hard is it to spot? Tricky and time-consuming but possible in some cases

Schools and businesses around the world are increasingly utilising email security software that automatically scans incoming mail by checking where the URLs in your email lead to. It does this to check the trustworthiness of your email, and in the process, registers as often multiple clicked links on your email tracking.

Again, it's important to stress that just because this software has scanned your URLs it does not mean that your email has been identified as junk or spam. It will likely have no impact on the campaign itself, only on the tracking or reporting.

Unlike email clients, the choice of which is usually down to the individual school or teacher, email security software like this is often implemented at local authority level, meaning that all staff working at all schools within a local authority could start registering as link clickers within your emails pretty much overnight.

Often, careful analysis of the campaign results can help identify these "bot clicks" due to one of the following patterns:

- Recipient has clicked on every single link (inc. all the social buttons in the footer)
- Recipient has only clicked the first link, even though it's not the main CTA
- Recipient has clicked one of the links multiple times (5+ is suspicious)

There are some steps you can take to mitigate these issues. For example, we insert a hidden "dummy" link at the top of our emails so that we can assume the only clicks on that link will be artificial ones. However, this is by no means foolproof as the behaviour of these systems can be unpredictable.

Likewise, it's perfectly possible for a teacher to have appeared to click a link in your email more than five times. Usually this is because they've forwarded it onto their colleagues – so ignoring teachers on this basis can mean discounting some of your best leads.



3. Apple's 'Mail Privacy Protection' App – Image Caching

How long has this been happening? This year

How Prevalent is this issue? Low but likely to increase very quickly

How hard is it to spot? Impossible

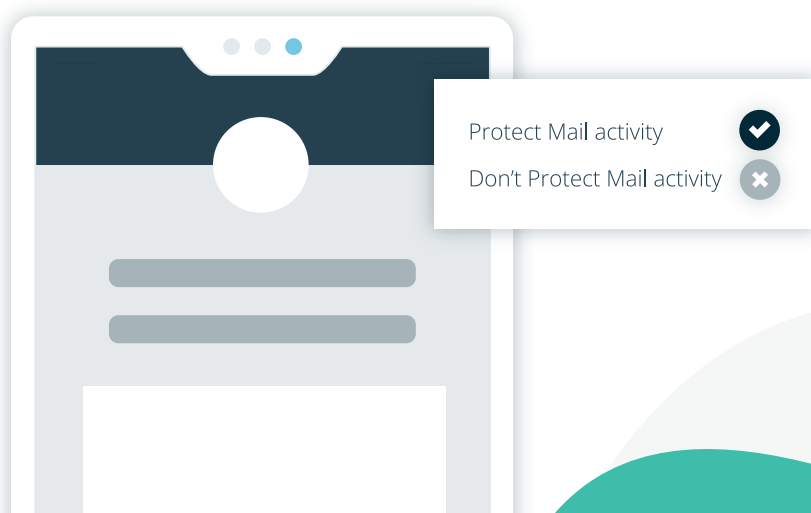
The latest blow to email tracking has been dealt by Apple, whose Mail Privacy Protection (MPP) has been developed in order to hide a user's IP address so that businesses can't link it to other online activity or determine their location.

The app works by downloading your email to the user's device before downloading all of the email's images and copying them to a new location on the Apple Privacy Cache. As we've already discussed, this downloading of images will then automatically register as an email open on your broadcasting platform.

This issue affects any email opened from the Apple Mail app on any device, and seeing as how Apple iPhone, Apple Mail, and Apple iPad account for over 50% of marketing email opens so far this year (the figure is 56% for the education sector) the issue is likely to represent a huge challenge for the entire digital marketing industry in years to come.

Note: When a user first opens the Apple Mail app they will be asked whether or not they want to "Protect Mail activity" or "Don't Protect Mail activity". So, it's not a default setting and we don't currently have any data around what % of users will choose the protect option.

At the time of writing, reports from around the industry – including at Sprint Education – suggest this is not currently leading to a huge distortion in open rates. However, the app is only available on iOS 15 which was released in September 20th 2021 so the impact is likely to become more prevalent as adoption of iOS 15 increases.



What does this mean for my email marketing?

Although email tracking can still provide some useful insights, education businesses must be extremely cautious about any strategic decisions they make off the back of a campaign's open and clicks.

The size of the impact this issue has on your business will depend upon how you currently use email tracking, but I've listed a summary of business areas you may need to revisit and re-evaluate:

1. **A/B Split Testing**

Anyone that carries out small split-subject testing to determine what the best performing subject line will be for a campaign is going to find that their results are less robust and open to distortion.

2. **Automated email sequences**

If you're using open and click data to determine what emails you send to teachers – either manually or via an automated sequence – then you need to be aware that these are not going to work so well. This is especially true when using opens – as many teachers you don't think are opening your email will be opening, just not downloading images, and many teachers you think are opening your email will not have actually opened it.

3. **Telephone or Direct Mail follow-ups**

It's also the case that if you're following-up email opens or clicks with a phone call or a postal campaign, you're either going to have to accept that you'll often be following-up the wrong people, or you'll have to spend some time visually checking and removing false engagers (we do the latter for our clients and it can be a time-consuming job).

4. **Making decisions about best times/days to send**

One of the things about Apple's new Mail Privacy Protection app is that it will download the images in an email at indeterminate intervals (ranging from immediately to several days later). Therefore the times/days when you're seeing email opens on your tracking are going to be very unreliable – especially when the app is adopted more widely in the future.

5. **Identifying which of your products or services are most in-demand**

Some email security software will almost always register a clicked link on only the first URL in your email. So, if your email is promoting several different products, or has a different CTA for primary vs secondary schools, you could be fooled into thinking that either one of your products is more in-demand than others, or that one type of school is more interested in what you offer. A resultant strategic business decision about which product or market segment to focus on could therefore be very ill-informed.



What can you do about it?

It's too early to say that email tracking is dead. However, it is time to re-evaluate what importance you place on it. In short, it's something that I'd recommend you analyse over a quick cup of tea and a biscuit, rather than while gathered around the boardroom.

Below is a list of actions you need to take away from this report:

1. Start focusing on other metrics instead of opens and clicks

Website analytics are a better indication of a campaign's performance than looking at opens and clicks. However, you need to look not only at how many visitors you're getting off the back of your email campaigns, but also how long those visitors are spending on your website. Remember, when email security software scans the URLs in your email that will register not only as a clicked link but also as a web visit (usually they will bounce very quickly and register no more than a few seconds on your website).

2. Use form submissions as the trigger for email sequences and workflows

I feel like almost every whitepaper or blog I've ever written ends up using the phrase "content is king" but who cares, I'm going to say it again. Content really is king. Make sure your number one marketing focus is on generating great content (free reports, lesson plans, resources etc.) and then use lead generation forms to capture the details of teachers that want to access that content. Then use these form submissions, which are 100% reliable, to trigger automated email sequences, programmatic mail, and other workflows.

3. Avoid placing too much importance on A/B testing subject lines or CTAs

Comparing open rates and click rates is still a valid exercise but avoid spending too much time split testing these things on small audiences before using the winners for your main campaign launch. It's highly likely that the open and click results you see from such a split test are going to be massively skewed by the factors highlighted in this report.

4. Don't sweat about optimum send dates and times

I've never been one to get bogged down in the best days and times to send. A great campaign will capture teachers' imaginations no matter when it's sent. When Apple's Mail Privacy Protection app becomes more widely adopted it's going to be impossible to track when a large portion of your audience has opened your email, so why not start letting go now?

5. Don't draw the wrong conclusions about email marketing in general

Finally, whatever you do, don't assume that just because email tracking can no longer be relied upon, this means that email marketing isn't in rude health. Over the past 12 months we've seen our clients generate [some of their best ever marketing results](#), including two that have seen over 1,000 form submissions off the back of a single email broadcast. Now, that's a metric we can all agree on!



Sprint Education

T. 01684 297374
E. info@sprint-education.co.uk
W. www.sprint-education.co.uk

