eff.org

# How To Turn PGP Back On As Safely As Possible

*Erica Portnoy and Danny O'Brien*

10-13 minutes

---

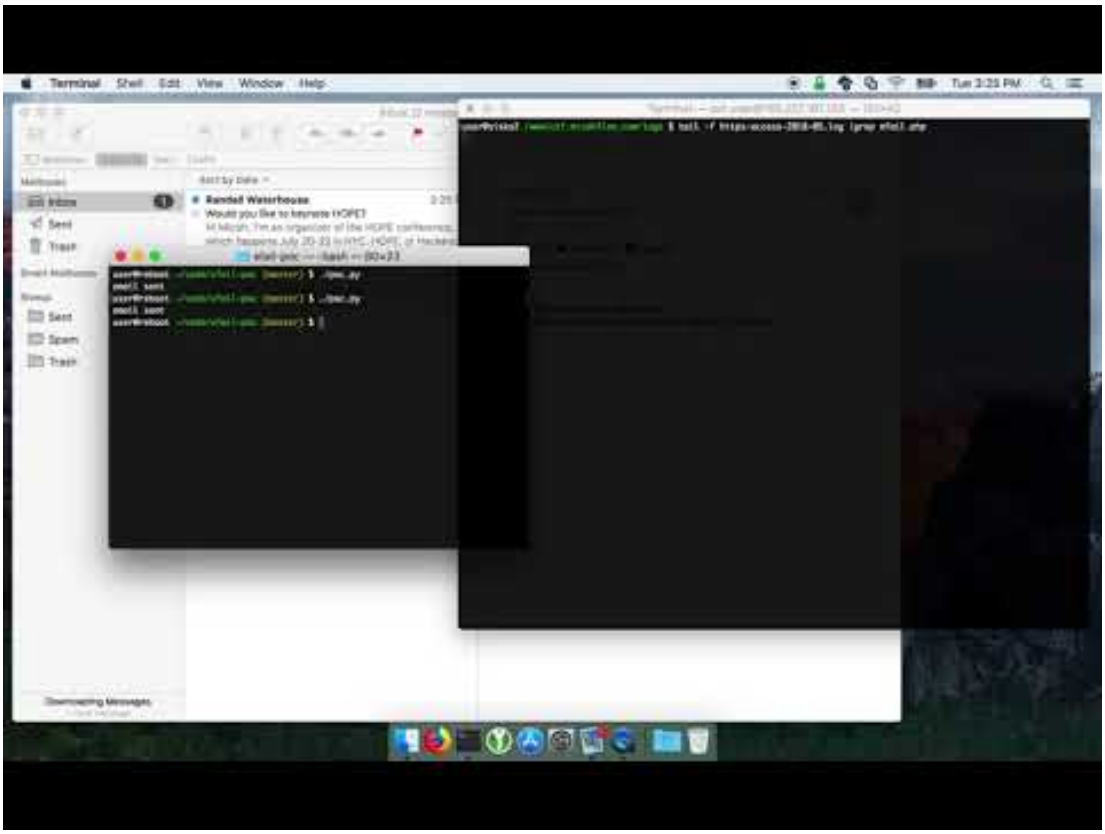
Previously, EFF recommended to PGP users that, because of new attacks revealed by researchers from Münster University of Applied Sciences, Ruhr University Bochum, and NXP Semiconductors, they should disable the PGP plugins in their email clients *for now*. You can read more detailed rationale for this advice in our FAQ on the topic, but undoubtedly the most frequently asked question has been: how long is *for now*? When will it be safe to use PGP for email again?

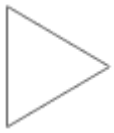
The TL;DR (although you really should read the rest of this article): coders and researchers across the PGP email ecosystem have been hard at work addressing the problems highlighted by the paper—and after their sterling efforts, we believe some parts are now safe for use, with sufficient precautions.

If you use PGP for email using Thunderbird 52.8 and Enigmail 2.0.6, you can update to the latest versions of Enigmail, turn on “View as Plain Text” (see below), re-enable Enigmail, and get back to using PGP in email.

For other popular clients: the answer is hazier. If you use GPGTools and Apple Mail, you should still wait. That system

is still vulnerable, as [this video from First Look's Micah Lee shows](#).





%3Ciframe%20allow%3D%22autoplay%3B%20encrypted-media%22%20allowfullscreen%3D%22%22%20frameborder%3D%220%22%20height%3D%22365%22%20src%3D%22https%3A%2F%2Fwww.youtube.com%2Fembed%2FIMPKe-GJSh0%3Fautoplay%3D1%22%20width%3D%22650%22%3E%3C%2Fiframe%3E

Privacy info.

This embed will serve content from

*youtube.com*

Other email clients have specific weaknesses reported in the EFAIL paper which may or may not have since been patched.

Even if they were patched, depending on how the patch was implemented, they may or may not still be vulnerable to other exploits in the class of vulnerabilities described in the paper. So be careful out there: keep your software regularly updated, and choose conservative privacy settings for the client you use to decrypt and encrypt PGP mail. In particular, we continue to not recommend using PGP with email clients that display HTML mail. If possible, turn off that feature—and if you can't, consider decrypting and encrypting messages using an external, dedicated application.

And remember, the safety of your messages also depends on the security of your correspondents, so encourage them to use clients that are safe from EFAIL too. You should even think about asking them to confirm which versions they're using to ensure it's safe to correspond.

**The Fixes in Detail**

The researchers' publication contains a proof-of-concept exploit that affected users who protect their communications with PGP. The exploit allowed an attacker to use the victim's own email client to decrypt previously acquired messages (or other protected information) and return the decrypted content to the attacker without alerting the victim. The attacker needed access to the previous (still encrypted) text. Unfortunately, an attacker that has access to your old encrypted emails is exactly the serious threat that the most targeted populations use PGP to protect against.

The attack, once understood, is simple to deploy. However, despite the fact that the vulnerability had been disclosed to the relevant developers months ago, many of the most

popular ways of using PGP and email had no protection against the attack at the time of the paper's publication. Because so many people in extremely vulnerable roles—such as journalists, human rights defenders, and dissidents —expect PGP to protect them against this kind of attack, we warned PGP users to hold off using it for secure communications and disable PGP plugins in their email clients until these problems were fixed.

That advice prompted a lot of discussion: some approving, some less so. We're talking to everybody we can in the PGP community to hear about their experiences, and we hope to publish the deeper lessons we, and others, have learned from EFAIL and how it was handled.

But for now, we've been concentrating on testing whether the exploit has been successfully patched in the software setups most used by vulnerable groups.

### Turning Off HTML vs Disabling Remote Content Loading

Many experts, after reading the research paper, were surprised we recommended disabling PGP in email, when it seemed like some less drastic options (such as turning off remote resource loading, and/or turning off their email client's ability to read and decrypt HTML mail) would have sufficed to fend off the most obvious EFAIL attack.

But upon closer reading of the text of the paper, it becomes clear that the researchers describe exactly how to circumvent mail clients' attempts to block the remote loading of resources. Other researchers have created, and continue to create, exploits that can defeat this supposed protection.

Further, with remote content turned off, a button is usually present to load remote content by choice. An alternative label for that innocuous-seeming button would be, “Leak all of my past encrypted emails to an attacker.” Having that button available to users is giving them an opportunity to shoot themselves in the foot.

Then there’s the other option for protection: turning off HTML in mail clients. At the time, the researchers were not confident that this protection *was* sufficient: they had already discovered a way of defeating S/MIME, a comparable email encryption standard, with HTML mail turned off. And while their simplest example used HTML to steal data, they also spelled out hypothetical attacks that might not need it.

Turning off HTML mail appears to be holding up as a defense. Unfortunately, not every client has this as an option: you can consistently turn off HTML in Thunderbird, but not in Apple Mail.

So, our first recommendation: whatever client you use, turn off HTML email. We have instructions for this in Thunderbird below.

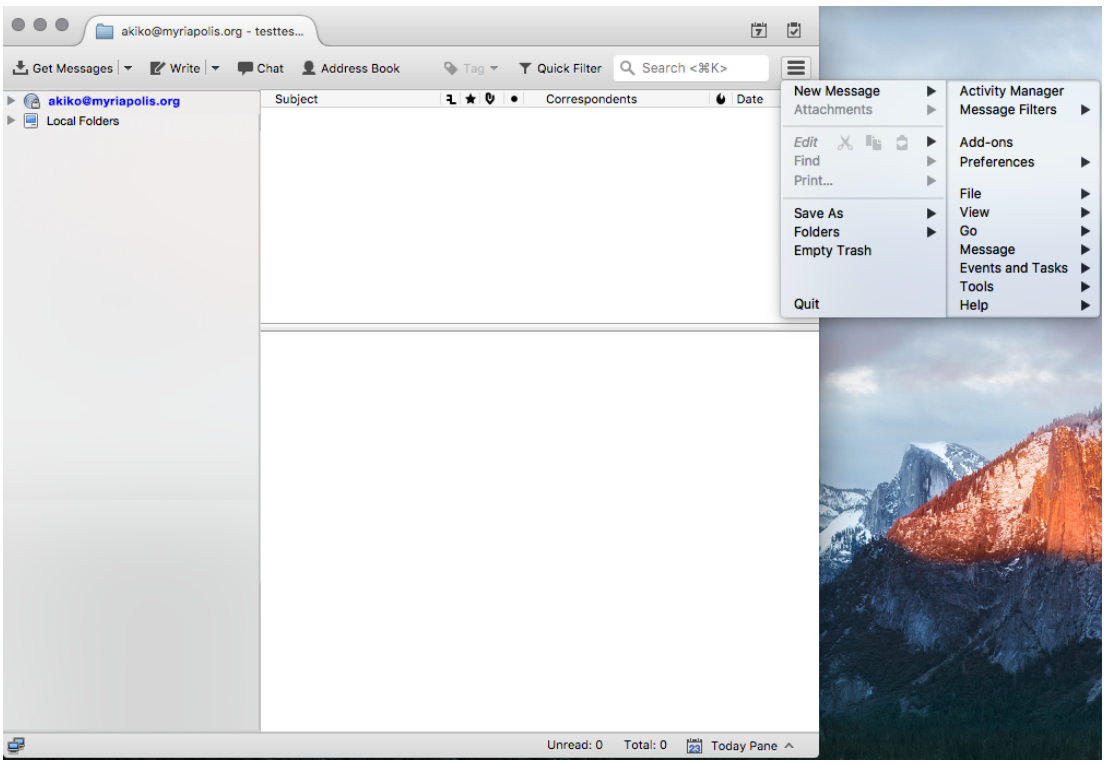
**Thunderbird+Enigmail Users Can Turn PGP Back On**

Thunderbird and Enigmail’s developers have been working on ways to protect against the EFAIL vulnerabilities. As of version 2.0.6 (released Sunday May 27), Enigmail has released patches that defend against all known exploits described in the EFAIL paper, along with some new ones in the same class that other researchers were able to devise, which beat earlier Enigmail fixes. Each new fix made it a little

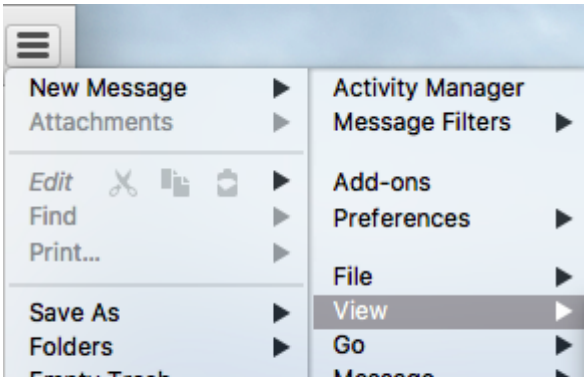
harder for an attacker to get through Enigmail's defenses. We feel confident that, if you update to this version of Enigmail (and keep updating!), Thunderbird users can turn their PGP back on.

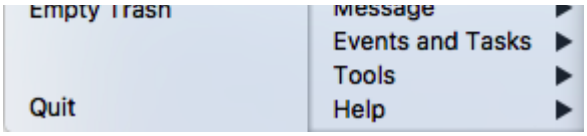
But, while Enigmail now defends against most known attacks even with HTML on, the EFAIL vulnerability demonstrated just how dangerous HTML in email is for security. Thus, we recommend that Enigmail users also turn off HTML by going to View > Message Body As > Plain Text.

1. First click on the Thunderbird **hamburger menu** (the three horizontal lines).

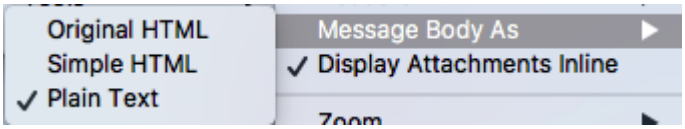



2. Select "**View**" from the right side of the menu that appears.






3. Select "**Message Body As**" from the menu that appears, then select the "**Plain Text**" radio option.




Viewing all email in plaintext can be hard, and not just because many services send only HTML emails. Turning off HTML mail can pose some usability problems, such as some attachments failing to show up. Thunderbird users shouldn't have to make this trade-off between usability and security, so we hope that Thunderbird will take a closer look at supporting their plaintext community from now on. As the software is now, however, users will need to decide for themselves whether to take the risk of using HTML mail; the most vulnerable users should probably not take that risk, but the right choice for your community is a judgment call based on your situation.

### Apple Mail+GPGTools Users Should Keep PGP Disabled For Now

Since Apple Mail doesn't provide a supported plugin interface, the GPGTools developers have faced a difficult challenge in updating GPGTools to defend against EFAIL. Additionally, Apple Mail has no option for users to view all emails without HTML (also called plaintext-only). Apple Mail only provides an option to disable remote content loading, which does not defend against existing attacks.

Despite the challenges with Apple Mail, the GPGTools

developers are working hard on fixes for all reported EFAIL-related attacks, and a release is expected very soon. That said, we do not recommend re-enabling GPGMail with Apple Mail yet.

### Other Clients

The EFAIL researchers did a great job reviewing and finding problems with a wide set of desktop email clients. Using one of the lesser-known clients may or may not leave you vulnerable to the specific vulnerabilities outlined in the paper. And depending on the way the patches work, the patches may or may not protect against problems discovered by future research into the same class of problems.

Our advice for all PGP email users remains the same: if you depend on your email client to decipher PGP messages, make sure it doesn't decode HTML mail, and check with its creators to see whether they've been working on protecting against EFAIL.

### The Future of Pretty Good Privacy

Unlike situations where a fix only requires one piece of software to be mended and upgraded, some of the EFAIL problems come from interaction between all the different pieces of using PGP with email: email clients like Thunderbird, PGP plugins like Enigmail, and PGP implementations like GnuPG.

There are lots of moving parts to be fixed, and some of the fixes involve changes to the very core of how they function. It's not surprising that it takes time to coordinate against

attacks that exploit the complex interconnections between all of these parts.

EFF has fought, in the courts and in the corridors of power, for the right to write, export, and use decentralized and open source encryption tools, for as long as PGP has existed. We're under no illusion about how hard this work is, or how underappreciated and underfunded it can be, or how vital its results are, especially for those targeted by the most powerful and determined of attackers. The transparent and public cooperation of all the parts of the PGP system make for some hard conversations sometimes, but that's what keeps it honest and accountable—and that's what keeps us all safe.

But if we're to continue to use and recommend PGP for the cases where it is most appropriate—protecting the most vulnerable and targeted of Internet users—we need to carry on that conversation. We need to cooperate to radically improve the secure email experience, to learn from what we know about modern cryptography and usability, and to decide what true 21st-century secure email must look like.

It's time to upgrade not just your PGP email client, but also the entire secure email ecosystem, so that it's usable, universal, and stable.