MOTHERBOARD
TECH BY VICE

# People Are Freaking Out That PGP Is 'Broken'—But You Shouldn't Be Using It Anyway

Hackers that can intercept your encrypted emails, or steal your emails from your computer or a server, may be able to decrypt them taking advantage of new vulnerabilities found in the way some email clients treat HTML.

By Lorenzo Franceschi-Bicchierai

May 14 2018, 6:44pm

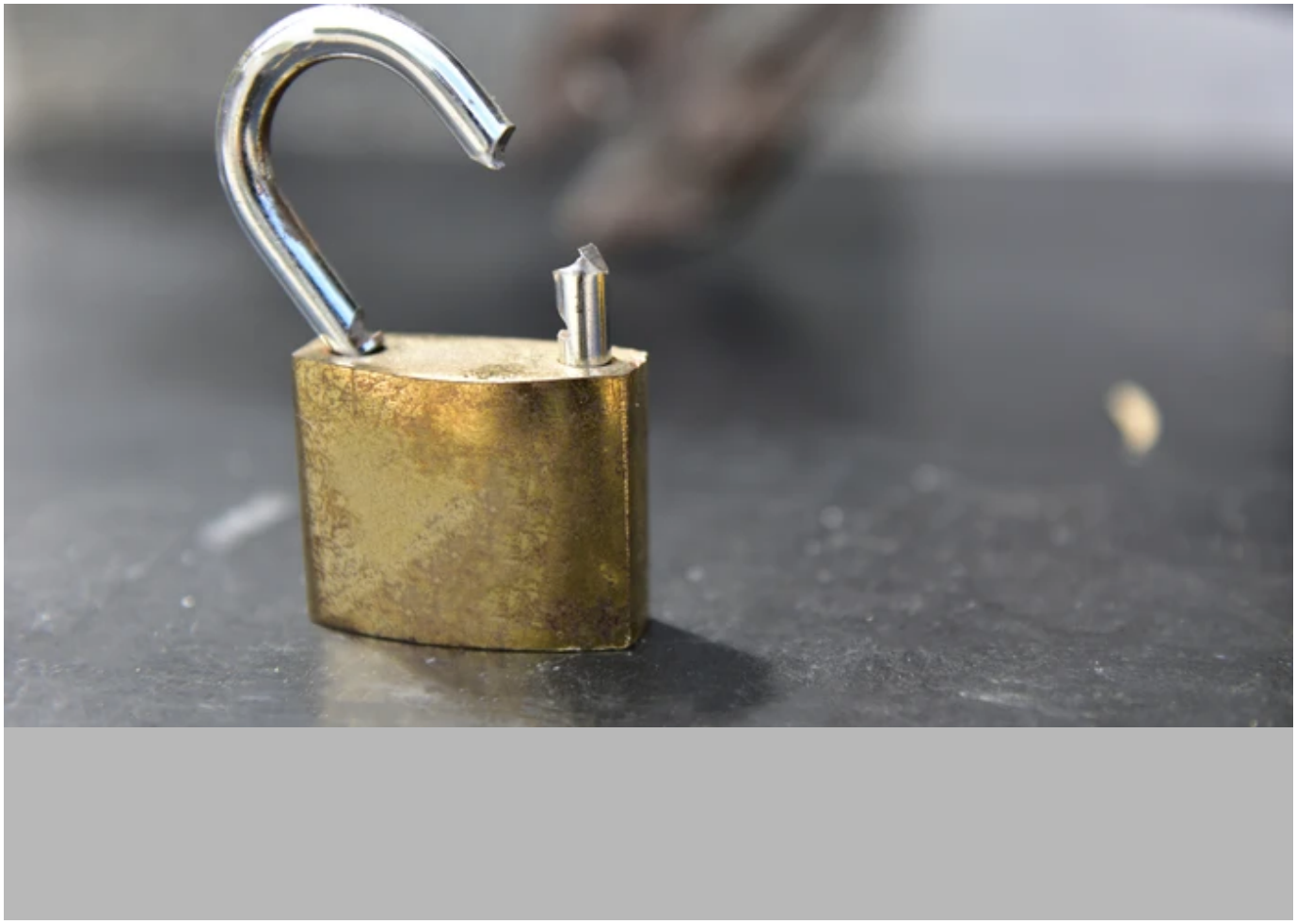


IMAGE: SHUTTERSTOCK

On Monday, the world was reminded once again that the almost 30-year-old encryption protocol PGP does still exist, and, yes, it still kinda sucks.

Mind you, the protocol itself is not really the problem. The crypto is solid. The problem is the way it's implemented, and the ecosystem around it. What's new is that a group of researchers has found a clever way for hackers to decrypt some PGP-encrypted emails.

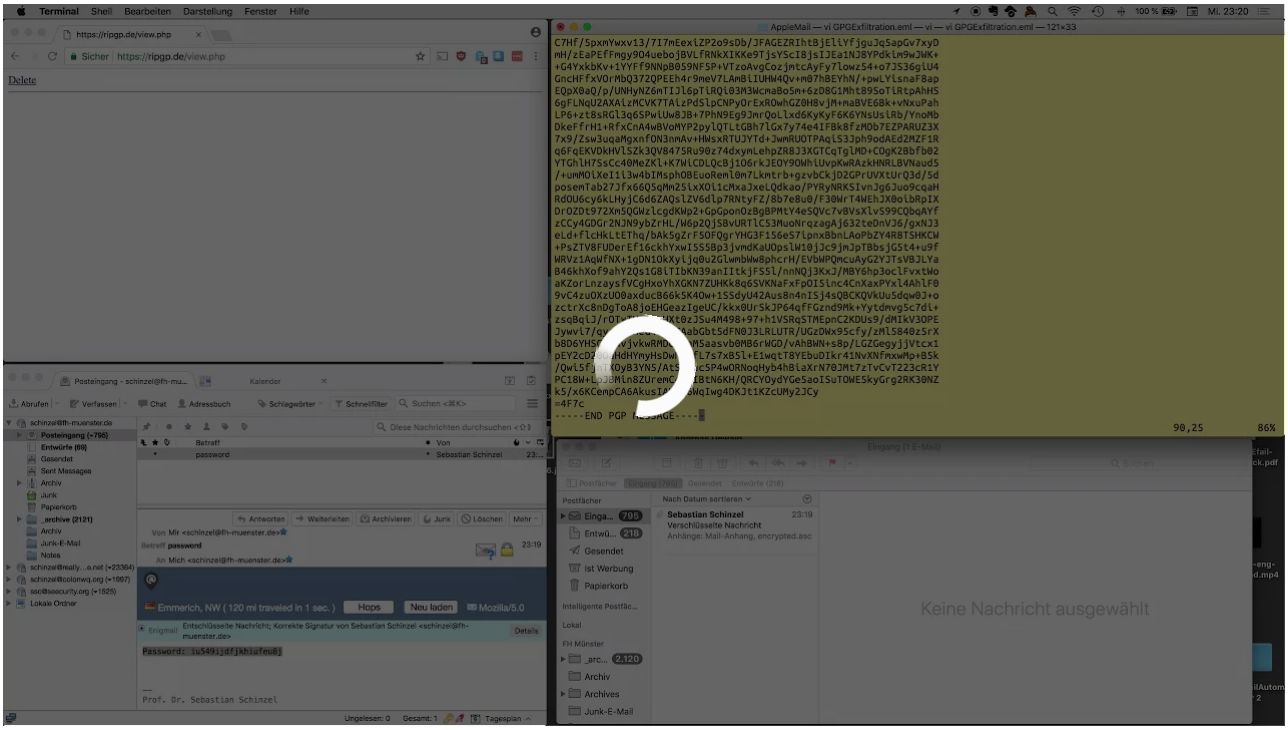
The researchers released **a paper** and published a summary of their findings on **a dedicated website** on Monday. The short version is that if an attacker can intercept your encrypted emails while they travel through the internet, or steal them from your computer, or from a server where they are backed up, they might be able to decrypt them. To do that, the hackers would need to modify those encrypted emails by inserting some custom HTML into them and then send them back to you. This technique, according to the researchers, tricks some email clients (such as Thunderbird, Outlook, and Apple Mail) and their PGP plugins (respectively Enigmail, Gpg4win, and GPG Tools) to send back the decrypted content of the original emails to the attackers.

> ***Got a tip? You can contact this reporter securely on Signal at +1 917 257 1382, OTR chat at lorenzo@jabber.ccc.de, or email lorenzo@motherboard.tv***

As Johns Hopkins University cryptography professor Matthew Green **put it**, this is "an extremely cool attack and kind of a masterpiece in exploiting bad

crypto, combined with a whole lot of sloppiness on the part of mail client developers."

The researchers recorded a proof-of-concept of what an attack actually looks like.



"The crypto-sky is not falling, but it is definitely serious," independent security and privacy researcher and consultant Lukasz Olejnik told me in en email, adding that these attacks affect "important bricks in the fragile encrypted mail ecosystem."

That's bad, but there's probably no need to panic.

For one, hackers need to first intercept or steal your encrypted emails. That's a relatively hard thing to do already, but it's a threat model PGP was specifically invented to mitigate. People who are being extra careful, like the Electronic Frontier Foundation, **are advising people** to use as little PGP as possible until email clients have released patches to stop these kind of attacks. (For what it's worth, GnuPG **released a statement** Monday saying if you have the latest version of Enigmail you should be fine.)

> ***Read more: Motherboard's Security Tuneup***

For **some experts**, dumping PGP completely may be too extreme. If you're worried about someone using this attack on your emails, disabling HTML rendering in your email client is a good way to mitigate risk. For sensitive communications, as we already noted in the **Motherboard Guide To Not Getting Hacked**, avoid using PGP. Not because of these attacks in particular, but because PGP has complicated implementations that make it prone to weird bugs, and it's hard to learn how to use it correctly.

Phil Zimmermann, the cryptographer who invented PGP, **stopped using it years ago**. Zimmermann told me in a phone call on Monday that he tried to use it once again a few months ago but was put off by the fact that his email client on MacOS wasn't able to import his old keys, for some reason.

"Email itself is kind of an old school kind of thing," Zimmermann told me.

PGP is old school too. There's of course some cases where PGP is a good way to share secrets or authenticate the person you're communicating with. But you should still avoid it if you can, and use other more secure means of communications such as Signal or Wire.

"Sadly I think what it tells everyone is that as standards age, legacy systems will almost inevitably be exploited," Alan Woodward, a professor at the University of Surrey, told me, "and email does not make for a good platform for secure messaging in the first place."



---

TAGGED: TECH, PRIVACY, ENCRYPTION, EMAIL, VULNERABILITY, BUG, INFOSEC, CRYPTOGRAPHY, PGP, CRYPTO, GPG, EFAIL

---