Why You Can Never Truly Delete Your Email

Think that clicking “delete” will actually delete your email? Think again.

When a user “deletes” an email in the normal fashion, it becomes invisible to that user and is immediately a candidate to be overwritten. But until it is in fact overwritten, it exists. And it may persist longer on company servers. So, even if it is taken off your computer, it may still be available on the host’s server.

Given that email-hosting companies are legally obliged to turn over user information to law enforcement and intelligence authorities with warrants—and these days even without them [1]—the impossibility of being certain of a deletion means you must presume that any email you compose will be available remain accessible forever.

“I think the most important thing for people to understand that you can't really ever delete anything,” Electronic Frontier Foundation staff attorney Hanni Fakhoury told the *Daily Dot*.

> “And when it comes to email, the provider may have a backup even if you delete it... (T)hat's why EFF is generally opposed to data retention policies [2], i.e., a government mandate for ISPs to keep digital records for specified periods of time.”

You do have some options to make your email harder to access, but doing so also makes it harder to use.

In EFF’s guide [3], “Don’t be a Petraeus: A Tutorial on Anonymous Email Accounts,”

the organization notes: “The current state of anonymous communication tools is not perfect, but there here are some steps that, if followed rigorously, might have protected the Director of the CIA, the Commander, U.S. Forces Afghanistan, and their friends against such effortless intrusion into their private affairs.”

The key words there are “rigorously” and “might.”

By combining encryption, an anonymous Web-based email account set up through a Tor browser or Circumventor tool that makes your personal IP address impossible to clock, you may remain out of reach of the increasingly overzealous authorities. It is important to note, however, that whichever email service you use may retain copies of any emails you send. That, combined with contextual information (personal information on your age, profession, location, etc.) might be enough for an investigator to identify you.

EFF points out that Hushmail allows users to set up email accounts while using Tor. Others discourage or forbid it. However, Hushmail, which guarantees that not even Hushmail employees are capable of compromising your anonymity, has forked over user information [4] with alacrity in the past.

Regardless of what kind of email setup you use, you are also encouraged to use “secure deletion [5]” software, such as Eraser [6], or to take a number of steps that truly delete the file in question.

The problem is that even when an email is actually deleted, and even if no copy of it has been retained on a company server, there are still elements that indicate the prior presence of the email. “[E]ven if a file has been securely deleted,” EFF warns, “its name will probably continue to exist for some time on your computer.” For instance, in Microsoft Word, the title of a document will persist in the Recent Documents menu, even if the email itself has been deleted.

The logins themselves are typically retained as well.

“Webmail providers like Google, Yahoo and Microsoft retain login records (typically for more than a year) that reveal the particular IP addresses a consumer has logged in from,” wrote the American Civil Liberties Union [7]'s Chris Soghoian [8].

Additionally, if there is any contact with that email by a computer whose IP address is visible, such as sharing an account with a recipient, that IP address can be the trail that unravels the whole conversation.

If you “give the account password to someone else who can then log in and view the message, obviously it doesn't matter if you disguised your IP address while visiting the site,” Bennett Haselton of Peacefire [9] told the *Daily Dot*. “The message is still sitting there and you've told someone else how to get it, so whoever they pass that info along to, will be able to access the message as well.”

“The thing is, email security in and of itself is a myth,” said Ian Lyons in a comment [10] on the New School of Information Security blog. Unless every single best

practice is followed to a T—and with large companies with less-than-tech savvy employees, that's nigh impossible—there will be breaches."

That's certainly something to consider the next time you pull up Gmail.

Read More [11]

December 10, 2012

Source URL (retrieved on *03/10/2014 - 4:49am*):
http://www.wirelessdesignmag.com/news/2012/12/why-you-can-never-truly-delete-your-email?qt-blogs=0&qt-digital_editions=0

Links:
[1] http://www.dailydot.com/news/senate-warrantless-email-ecpa-privacy-amendment/
[2] https://www.eff.org/issues/mandatory-data-retention
[3] https://www.eff.org/deeplinks/2012/11/tutorial-how-create-anonymous-email-accounts
[4] http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/
[5] https://ssd.eff.org/tech/deletion
[6] http://www.heidi.ie/node/38
[7] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CEAQFjAA&url=http%3A%2F%2Fwww.aclu.org%2F&ei=GnTCUIKKFsjmigLJzYDYCg&usg=AFQjCNFkW0bpKZYAqodZrAfRg3ZiGyNpkA
[8] http://www.aclu.org/blog/technology-and-liberty-national-security/surveillance-and-security-lessons-petraeus-scandal
[9] http://www.peacefire.org/
[10] http://newschoolsecurity.com/2012/11/email-security-myths/#comments
[11] http://mashable.com/2012/12/10/email-can-never-be-deleted/