Texting or e-mail: Which gives you more secure communication?

October 14 2019, by Jefferson Graham, Usa Today

Credit: CC0 Public Domain

WhatsApp, text or email—which is the most secure option when your conversation really has to be locked down?

The recent private-messages-going-public news with Congress scouring the messages obtained from diplomats as part of its impeachment inquiry again has private exchanges top of mind and offers a good jumping-off point to discuss what options you have with the tools you use most.

There are varying degrees of privacy or protection among the chat and communication platforms. Ultimately, there are precautions you can take.

Encryption, says Apple on its website, is used to protect trillions of online transactions every day, for shopping, paying bills and communicating with programs like its own iMessage or FaceTime, or Facebook's Whatsapp. Encryption, says Apple, "turns your data into indecipherable text."

And this has been a hot topic in Washington. Attorney General William Barr wrote to Facebook, asking it to change its encryption policy for Whatsapp.

"We must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity," Barr said.

Facebook opposes Barr's request.

Meanwhile, how to encrypt your communication?

Start with e-mail

Messages written via popular web programs like Google's Gmail, Microsoft's free version of Outlook or Yahoo Mail are not encrypted by default, nor is government or corporate e-mail. (There are ways to send encrypted Gmail, but only to other Gmail users, via a third party plug-in.) The free webmail programs are both easy to track, both by subpoena and by the companies offering the free tools, says Micah Lee, director of information security for the Intercept website. "E-mail is the easiest to spy on," he says.

That said, there are a handful of startups offering encrypted e-mail, including Switzerland-based Proton, while Microsoft offers the ability to encrypt Outlook (for paying subscribers), but it's complicated. You essentially turn it into gibberish and send a "digital key" to the recipient to unlock it and make it readable.

So you want to turn to the phone and secure text messages

"But you shouldn't use a company device," says Lee. "Many of these have corporate spyware and can take screenshots of what you're doing. Only use your personal phone."

If your personal phone is a Samsung, it offers a feature to encrypt data after it's been generated and have it stored on an external SD card for Galaxy phones. To use this feature for text messages, download the Messages app for Android and move them there. Know that once you encrypt the data, you're able to decrypt the data only on the same device. Samsung notes that you won't be able to read it anywhere else.

Additionally, the iPhone has a feature that can prevent outside forces like law enforcement or the government from using a USB device to tap into your phone and grab your unencrypted data. Go to Settings, Touch ID & Passcode, and scroll to the bottom for USB Accessories, to click off and prevent USB accessories from connecting when the iPhone has been locked for more than an hour.

Traditional SMS text messages on your phone

Texts sent on the iPhone, the most used digital device in the United States, to another iPhone, are encrypted, and thus, wouldn't be able to be read without decoding, according to Apple. The company says text messages stored on its iCloud service will be encrypted as well, as long as the user has opted in for two-factor authentication sign-ins. Note that if the person on the other end doesn't have an iPhone, the message is no longer encrypted. (Android phones don't encrypt SMS messages by default, says Lee, but as we noted, backing them to an external card and opt to encrypt the data manually.)

Encrypted chat apps

Signal, Wire, Rakuten Viber and Whatsapp are popular apps to look to for secure encrypted written and spoken conversations. Yes, the same Whatsapp that's owned by Facebook, the company that's apologized many times for security breaches.

Because Whatsapp is the most popular chat program in the world, used by over 1 billion users, the odds are high that the person you want to speak to currently uses it. That's a huge bonus for being able to communicate freely and privately, says Lee. And it makes a big deal on its website about how messages are encrypted and not read by company officials.

However, Facebook does have access to your metadata and can determine who you spoke to and when, adds Lee.

—The app Signal does not have Facebook ownership issues and is considered the go-to app for the most secure form of communication. Even Edward Snowden, the former U.S. whistleblower who has been hiding in Russia since 2013, offers a testimonial on Signal's home page.

"Signal messages and calls are always end-to-end encrypted and painstakingly engineered to keep your communication safe," the company says. "We can't read your messages or see your calls, and no one else can either."

Signal says it doesn't accept advertising and is supported by grants and donations.

—Germany-based Wire says it provides the "strongest security" for organizations and their workers, but it's not free, starting at around $6.50 monthly. "End-to-end encryption gives you the confidence to talk, message, and share across teams and with clients, through a single app that's available on all of your devices," the company says.

—Rakuten Viber, based in Japan, points out on its website that it offers a "Secret Chats" feature that lets users set a self-destruct timer, so just like on "Mission: Impossible" or SnapChat, after the message is read, "it is automatically deleted from the Viber chat."

Facebook Messenger

These messages are not encrypted by default, but they can be. Facebook offers a feature called "Secret Conversation" for private chatting, but both sides have to turn it on for it to work. (Click the word "Secret" at the top right side of the screen on iPhone or the lock icon in the same place on Android.)

Authenticity can be proven during the conversation by both sides checking their digital ID keys (stored under the person's names) and making sure they match.

But privacy is in the eye of the beholder, as the person on the other end of this encrypted conversation can easily make a screenshot and share it with the world.

Still, Facebook says the messages are intended "just for you and the other person—not anyone else, including us."

Meanwhile, Lee understands why the diplomats may have opted for texting. "It's quicker and more convenient. Who wants to wait for the e-mail to arrive?"

Citation: Texting or e-mail: Which gives you more secure communication? (2019, October 14) retrieved 25 April 2024 from https://techxplore.com/news/2019-10-texting-e-mail.html