SECURITY

How to Encrypt All of the Things

Want to keep outsiders from listening in on your chats, phone calls, and more? Encrypt them. All of them.

The best way to encrypt data at rest—rather than messages in motion—is en masse, by encrypting compartments of your storage, or simply encrypting your entire hard drive.AARON FERNANDEZ

CRYPTOGRAPHY WAS ONCE the realm of academics, intelligence services, and a few cypherpunk hobbyists who sought to break the monopoly on that science of secrecy. Today, the cypherpunks have won: Encryption is

everywhere. It’s easier to use than ever before. And no amount of handwringing over its surveillance-flouting powers from an FBI director or attorney general has been able to change that.

Thanks in part to drop-dead simple, increasingly widespread encryption apps like Signal, anyone with a vested interest in keeping their communications away from prying eyes has no shortage of options.

In fact, secure communications are not only attainable but perhaps even the new default, says Matthew Mitchell, the founder of security training organization Crypto Party Harlem and an adviser to the Open Technology Fund. “Security is here to stay. It’s now expected that a product just encrypts without you having to do anything,” Mitchell says. He describes every unencrypted internet-connected app or web tool as a window without curtains. “Now people are learning there are curtains.”

Still, effective encryption doesn't always just *happen*, especially once you move beyond basic messaging. Here's how to keep snoopers out of every facet of your digital life, whether it's video chat or your PC's hard drive.

Text Messaging

Signal, the smartphone and now-desktop encryption app, has become the darling of the privacy community, for good reason. It’s as easy to use as the default messaging app on your phone; it’s been open source from the start, and carefully audited and probed by security researchers; and it has received glowing recommendations from Edward Snowden, academic cryptographers, and beyond. Its cryptographic protocol also underpins the encryption offered by WhatsApp and Facebook's Secret Conversations. (Those two services don't, however, offer Signal’s assurance that it doesn't log the metadata of who is talking to whom.) The most important note, for encrypted chat newbies: Remember that the person with whom you're messaging has to be on the same service. Signal to Signal provides rock-solid end-to-end encryption; Signal to iMessage, or even to WhatsApp, won't.

There are plenty of other ways to communicate securely. Unlike Signal, messaging apps like Wire, Threema, and Wickr allow you to sign up without tying your account to a phone number, a significant feature for those seeking some level of anonymity in addition to security. And iMessage has also quietly offered end-to-end encryption for years, although without the assurances Signal offers about no logging of metadata, or that messages aren’t being intercepted by spoofed contacts. (Signal is designed to warn you when the unique key of your contact changes, so that he or she can’t easily be impersonated on the network.)

On the desktop rather than the phone, a few emerging tools offer advantages over Signal too: Keybase, Semaphore, Wire, and Wickr Pro offer some approximation of an encrypted version of the collaboration software Slack, with more collaboration and team-focused features than Signal offers. And desktop instant messaging app Ricochet uses Tor's onion services to allow true peer-to-peer messaging that's anonymized, encrypted, and directly sent to the recipient, with no intermediary server that might log conversations, encrypted or not.

Video and Voice

Have you heard of Signal? Perhaps several times in the earlier paragraphs of this story? Well, it enables encrypted video and voice calls too. WhatsApp again uses Signal's encryption protocols for voice and video, but as with text messages, doesn't promise not to keep logs of conversation metadata. Apple's FaceTime integrates end-to-end encryption by default, but with the same caveats about metadata and, as with iMessage, without Signal's protections against spoofed contacts.

Encryption app Wire, cofounded by one of the original engineers behind Skype, also offers video calls and one very useful voice feature Signal doesn't: Multiperson voice calls. Create a group, hit call, and everyone's phone rings—with the assurance that conference call's secrets will be protected (assuming no one is dialed in from a crowded coffee shop).

Storage

The best way to encrypt data at rest—rather than messages in motion—is en masse, by encrypting compartments of your storage, or simply encrypting your entire hard drive. Apple's Disk Utility allows you to encrypt chunks of your internal storage or external drives. As Mac security firm Intego describes here, you can either create a new encrypted "image" on your hard drive, or turn an existing folder into one of those encrypted hard drive compartments. Veracrypt does the same for both Macs and Windows.

On Windows, Bitlocker allows you to take that encrypted storage to its logical conclusion, encrypting your entire disk. Apple's Filevault does the same for Macs; just switch it on under **System Preferences > Security and Privacy**,

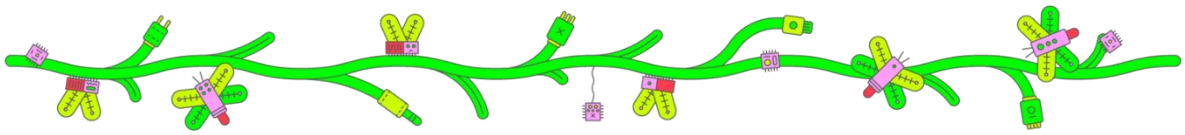
restart your Mac, and you'll have full-disk encryption. For both those utilities, it’s important to remember that they provide their strongest protection when the computer is fully powered off; when it's on, it stores keys in memory, a potential risk.

Encrypting your smartphone's storage is even easier—in fact, practically effortless—with modern Android phones and iPhones, which use full disk encryption by default. Just set a strong, hard-to-guess passcode at least six digits long. For added security, don't use biometrics like fingerprint or facial recognition systems, which can be more easily defeated than strong passcodes. And on Android, don't use a pattern unlock, which can be easily spotted by someone glancing at your phone or even cracked by analyzing your screen smudges.

Email

Although some old-school encryption stalwarts still insist on sending emails encrypted with the 25-year-old landmark privacy software PGP, email is far from the most convenient way to send secrets today. But for those who insist on that medium, some applications are designed to bolt a layer of secrecy over old-fashioned email. Enigmail, for instance, integrates with Mozilla’s Thunderbird email client, and the Mailvelope browser plugin encrypts messages in Gmail. Email service Protonmail offers its own end-to-end encrypted email platform, but emails are only fully protected between Protonmail users.

In an era where seamless encrypted messaging abounds—and is both easier and likely more secure than email—you might as well ditch that antiquated protocol altogether. Instead, choose from the multitude of encrypted messaging apps and upgrade your conversation’s speed while you’re locking down its security.



The Wired Guide to Digital Security

- **More Tips for Public Figures**: After you've encrypted everything, sign up for Google Advanced Protection, take a tour of Tor, and deploy physical measures to increase your digital security.
- **Tips for Regular Users (the Hackers are Still Circling)**: Master passwords, lock down your smartphone, keep yourself secure from phishers, know how to deal with getting doxed, and, if you have kids, keep them safe online.
- **Professionals Are After You. Time to Get Serious**: If you think they're onto you, remove the mic from your devices, find bugs, and (worst case scenario) dive down the paranoia rabbithole.

Andy Greenberg is a senior writer for WIRED, covering security, privacy, information freedom, and hacker culture. He's the author of the book *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. The book and excerpts from it published in WIRED won a Gerald Loeb... Read more

SENIOR WRITER

-