Welcome to Securing Your Digital Footprint-

Securing the least secure communication form - Emails

It may come as no surprise anymore, but your email isn't private. In fact, it's one of the least secure methods of communication you can use. In contrast, phone calls typically aren't recorded and stored, and even if they were, your employer and law enforcement would have to go to court to gain access to them.

Emails are stored at multiple locations: on the sender's computer, the Internet Service Provider's (ISP) server, and on the receiver's computer. Deleting an email from your inbox doesn't mean there aren't multiple other copies still out there. Because they are digital, they can be stored for very long periods of time. You may want to think twice before emailing something you don't want others to see. Source.

Not only do we have to worry about the gov't reading our emails, recently a Google employee, parent company of Gmail, was fired for snooping - reading users emails. Then there is the data mining of *your* data - where the content of *your* emails are scanned and then targeted ads are placed in *your* inbox. Creepy! Who knows who they are selling or 'sharing' *your* info with?

The Fourth Amendment, the Electronic Communications Privacy Act and the Patriot Act

The laws around email privacy begin with the Fourth Amendment and are governed by the "reasonable expectation of privacy" standard. Unfortunately, given the open nature of email mentioned above (passing through several computers and stored at multiple locations), the expectation of privacy may be less for email, especially email at work, than for other forms of communication.

Emails are also governed by the Electronic Communications Privacy Act (ECPA) and the Patriot Act. Although the ECPA originally set up protections (such as a warrant requirement) to protect email, those protections have been weakened in many instances by the Patriot Act. Even where the protections remain under the ECPA, emails lose their status as a protected communication in 180 days. The Stored Communications Act (SCA) is a law addressing voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA). The way the US government interprets the SCA means that any emails older than 180 days are seen as abandoned. This means if you leave messages in your Gmail or Hotmail account, or even on your business hosted Exchange server, they become available for any law enforcement agency without a warrant, or even probable cause. All they need do is ask Gmail or Hotmail, since those messages are no longer yours.

It is much harder for local law enforcement (LLE) to get a warrant to access your personal stuff at home, than it would be from your employer. Source.

How to Keep Your Email Private

To maintain "your expectation to privacy" always use password-protected computers and email clients. After that, there's really only one way to ensure that your emails are kept confidential -- encrypt them. This is discussed in the article on PGP Encryption.

Make sure you download your emails, onto your own computer. Apple's Mail program will allow you to do this:

1. Open Mail
2. Click on preferences
3. Click on your email account(s)
4. Click on 'Advance'
5. Click the options to move your mail to your own computer.

One of the drawbacks to Apple's Mail program, once you enter your email account(s) and get them working, is the program stays open and doesn't require a password. One way to increase security is to use Keychain Access, which comes with your Mac, to lock the screen with a password.

1. Applications
2. Utilities
3. Keychain
4. Preferences
5. Under the 'General' tab click the "Show shortcut in Menu Bar" button
6. You will see a lock in the menu bar, if you click on it a context menu opens up
7. Click on 'lock screen'

Too much hassle? Download a program to do it for you.

Or, if you have a shared computer, create multiple users accounts.

1. System Preferences (right click on the apple top left of your screen)
2. Users and groups
3. If your padlock is closed you will need your computer password to open it
4. Click on the '+'
5. Type of user
6. Name of user
7. Add a password

In addition to PGP you can move away from Gmail, Hotmail, and Yahoo. This, as it turns out, is easier said than done when they become the 'it' service.

Free email services you may want to consider: Zoho, mail.com - not the same program as Apple’s Mail, GMX owns mail.com, inbox.com, Yandex - hosted in Russia, and Shortfall.

Update:

Until recently Protonmail was a paid service. But if you are looking for an easy to use, encrypted option that works with iOS(iPhone, iPads), Android and on the desktop through a browser this is the ticket.

The following are not recommended: Outlook - replaced hotmail, Yahoo, and Facebook mail.

Notice I’m not recommending the ‘big/main players?’ That's because the point is to move to a service that isn't already in bed with government. Of course, if anyone is presented with a court order they will have to comply.

If you love Gmail and don’t want to leave, use a program that puts encryption in your browser. Mailvelope encrypts email and works with Firefox and Chrome. There are doubts on how well this will work as users leave the job of encryption to the browsers. Both Firefox and Chrome LOVE to track you, I’m sure you’ve all noticed after doing a specific search for something, the next day ads for that specific thing shows up in your inbox?

Another option, if you have a website, mydomain.com, you have email through your hosting company, info@mydomain.com. Used from the dashboard of your hosting company or through a free email application like Mozilla’s (Firefox) Thunderbird https://www.mozilla.org/en-US/thunderbird/ or Apple’s Mail program, you will need these programs in order to get PGP installed. Once you’ve setup the particulars of your hosted email, using one of these programs makes accessing your mail easy.

Like the sound of this but don’t have a website? A year of hosting plus a **domain name** is around sixty dollars a year. If you don’t want to go that route, there are hosting companies that will do just email. Look for the hosting companies offering SSL and IMAP/POP access. Runbox, http://www.tuffmail.com/packages.php, is only six-dollars a month.

No matter which options you choose to secure your email from prying eyes. Feel more confident in your communications. However, don’t get complacent, I will provide updates to the information. We live in an insecure digital age. With some extra effort you can keep your email reasonably safe.