An EquiHacks Primer

For nearly two months, Equifax, one of the nation's Big 4 credit ratings agencies left the personal information of 143,000,000 unsecured. If you have a bank account, loans, have ever received a credit card offer in the mail, or even worked a documented job, your information is likely compromised.

How can you respond?

First, get a copy of your credit report at annualcreditreport.com. Don't use other sites, they aren't actually free. AnnualCreditReport is the only site authorized by the US Government to provide you access to the Big 3's credit files. Keep this report as an archive, you will need it to contest any fraud you might encounter in the future.

Next, freeze your credit reports. A credit "freeze" or "lock" merely prevents other agencies from pulling your credit score or opening new lines of credit in your name, without your approval. This change will not impact your current debts or savings and you will be able to temporarily "thaw" your report, in order to apply for jobs or housing.

In Massachusetts, freezing, thawing, or requesting a replacement PIN costs $5 per credit agency, leading to a total cost of $20 to freeze all accounts. For victims of identity theft, including spouses of victims of identity theft, freezing and thawing is free if you provide a copy of a valid police complaint.

Call these numbers to freeze your report:

TransUnion: 888-909-8872
Experian: 888-397-3742
Equifax: 800-349-9960
Innovis: 800-540-2505

Sign up for fraud alerts: Individuals who have experienced identity theft in the past, who have a police report, are qualified for free extended fraud alerts, which doubles the number of free credit reports you can request in a year, among other safeguards.

You can also opt out of junk mail and pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). This remains valid for 5 years, although you can mail in a form to be permanently removed from unsolicited credit offers.

Brought to you and paid for by the Massachusetts Pirate Party

We believe you should have privacy and the government shouldn't. You can find us online at **masspirates.org**, and on Twitter, Facebook and YouTube via https://<site>/masspirates.

Protect Your Privacy On-line

Concerned about your privacy and security, especially on-line? Don't be paranoid and lock it all down or throw up your hands and say everything is public anyway. Here are some helpful things you can do to protect yourself:

First, think of what threats you are most concerned about. If you are 15, your parents are high on your list. If you are 30, it could be identity thieves, your boss, an ex-lover, or even a roommate.

Second, make a list of the data and devices you want to keep private from the threats that concern you and make a list of counter measures you can use to protect yourself. Here are a few more things you can do:

Password Management: Think pass phrases not passwords. The longer and more random the better. Never use a single word or common password like password or 1234, since those are easy to crack. If you need to remember your pass phrase, pick four or five random words and turn them into a phrase. **NEVER repeat the same pass phrase with different accounts or devices.**

Use a passphrase manager app that creates encrypted files or even a notebook that is always with you. Pass phrase/word managers save your passwords in an encrypted file that you unlock with its own pass phrase. They can also generate a long random passphrase for you.

Account Management: Besides using good pass phrases, turn on two factor authentication (2FA) if the service supports it. 2FA requires that you enter your userid, password and a random number that is either sent to you by a text message or generated on an app you own, like **Authy** or **Google Authenticator**.

Encrypt your devices: Always enable a pass phrase or pin for your device and turn on file encryption so it is difficult for anyone to get your data. File encryption works best when your device is off or before you login after a restart. Encryption for iOS is on by default. You need to enable disk encryption for Android, Windows, MacOS and Linux.

Use encrypted tools to communicate:

- **Signal** (https://signal.org) is a free, easy to use app for iOS/Android and Chrome on desktops that encrypts your text messages, phone calls and video chats to other people using Signal. It retains very little information about who you are contacting.
- **Tor** (https://torproject.org) is a free web browser that helps you be anonymous when you browse websites. It connects to a network of other Tor nodes to hide your traffic. It isn't fool proof and don't use Tor to access accounts that you use outside of the Tor network.

Come to one of our cryptoparties to learn of other ways to protect yourself or ask others for help. Find upcoming cryptoparties at **cryptoparty.in/boston** or join out mailing list at
lists.mayfirst.org/mailman/listinfo/cryptoparty_masspirates.org/