Digital Personal Security Primer

Author	josh
Date	2020-06-05 12:16:21

Overview

Computers in all their forms (PC's, tablets, mobile phones, and more) are an integral parts of our lives - from work, to hobbies, to activism. It is as critical to protect your digital life as it is your own home. With many attackers and attack vectors, there is NO one size fits all security model for any individual, but there are some basic practices that can help most everyone.

Let's learn some important tips for managing your online life - passwords & password storage, 2 factor authentication, and encryption.

Basic Practices for Everyone!

Passwords and Password Storage

A basic security item everyone needs to get right is passwords. Insecure passwords are a first line of failure in a lot of data breaches, and can wreck your digital security from the get go.

> Create lengthy, secure pass*phrases* rather than passwords. Think of a unique and hard to guess sentence - the more characters, the more exponentially difficult it becomes for an attacker to guess. "ThisIsMyPassphraseForAccount" is much, much better than "bday0105" for example.
>
> This is because passwords are generally not stored in plain text (the actual password) but rather stored as a *hash* - you can think of it as a one way form of "encryption" although that's not exactly what it is technically. Brute force "reversing" becomes much more difficult with a longer passphrase.
> Do NOT reuse passphrases. Create a unique one for each important account. That way if one is compromised, the rest of your accounts can remain safe.
>
> Often an attacker will breach your passphrase from a more insecure site and use it to get into more important things like banks, emails, etc. because of password reuse.
> Store your passphrases in a secure, encrypted password manager. Use an open source tool such as KeePass to store passphrases and even generate secure random ones. These tools take one secure "master" passphrase, so you don't have to remember each individual account.
>
> If you want a simpler solution, LibreOffice (Open Source alternative to MS Office) supports secure encryption for documents using AES-256 encryption. You can create a spreadsheet of credentials and encrypt them with a simple wizard.
>
> Do NOT use MS office for the same purpose; older versions do not use encryption for

password protection and are easy to break. I have not yet confirmed that the latest version use encryption, but I know LibreOffice does

2 Factor Authentication

2FA is another critical part of securing accounts with a second layer of verification that you are who you say you are. 2FA codes are "something you have" and your password is "something you know"

- Turn on *Authenticator-based* 2FA on any accounts you can. These use an app like Microsoft Authenticator, Duo, etc. This is more secure than text-messaged based 2FA which can be compromised with SIM swap attacks.
- Never, ever give 2FA codes to someone claiming to be from a company's support team, etc. There's no legitimate reason to ever give up this information

Encryption (Documents and Messages)

Secure encryption is critical for protecting your information from unauthorized parties, including the state. Proper encryption cannot be reversed without the passphrase/key, and in most US jurisdictions you cannot be forced to give up encryption keys as far as I am aware (NOT a lawyer). At any rate, encryption also protects you from device thieves and hackers trying to steal your information.

- Turn on *full disk encryption* for your devices! For a mobile phone like an Android, you can require an encryption PIN on startup. For PC's, use VeraCrypt for Windows or the built-in full disk encryption on popular Linux distributions.
- Don't communicate any critical information over email or SMS text messages. Use a secure, open source encrypted messaging app such as Signal
- As stated in the password section above, use a securely encrypted password manager to store your credentials - no unencrypted files and no post-it notes, please!

Security Starts with the Basics

Security is a deep and ever-changing topic. These are simply some basic tips that can help anyone start securing their digital life against attacks from a wide variety of threats - thieves, trolls, and even the state.

Be safe and make your voices heard, everyone!