Internet and Data Extended Security Guide

Authors: Holochain, Greg Cassel

- Personal Security Principles
  - Avoid Sharing Confidential Information
  - Use Strong Passwords
  - Don’t Access Sensitive Information on Unprotected Devices
  - Don’t Leave Sensitive Information Lying Around
  - Report Suspicious Activity to our Data Security Team
- Introduction to Passphrases
  - Strategy 1: Use a password manager
  - Strategy 2: Use four (or more) common words, selected at random (see this webcomic)
    - Examples of strong passphrases
    - Examples of poor passphrases
- Personal Security Checklist
  - 1. Set a strong passphrase/word and auto-lock on all your devices
  - 2. Set a strong passphrase/word on your team chat account
  - 3. Set strong passphrases/words on all team-hosted accounts you use
  - 4. Set strong passphrases/words on all of the team communications channels you use
  - 5. Turn on two-factor authentication for all your important accounts
  - 6. Store your passwords securely
  - 7. Turn off your browser’s “save passwords and info” features
  - 8. Clean up your cloud drives and publicly-hosted files
  - 9. Check security settings on shared work files
  - 10. Make sure your GitHub/GitLab SSH key includes a passphrase
  - 11. Get a cheap burner phone to receive two-factor authentication texts on
  - 12. Put tape or webcam cover over your camera
  - 13. Use a VPN all the time, especially on public wifi networks
  - 14. Use a hardware wallet for all your cryptocurrencies
  - Finally: Get Help

Personal Security Principles

Avoid Sharing Confidential Information

- Never give out our company or customer information to unauthorized users, including unsolicited emails or phone calls.
- Hackers can be very convincing and have a lot of tricks up their sleeves. Always be wary of suspicious activity, especially in regard to confidential or sensitive information.
- Never email usernames and passwords to anyone, not even yourself.
- Be cautious of suspicious messages that supposedly come from sources like PayPal, Amazon, or a bank.

Use Strong Passwords

- Don't use the same password for multiple accounts.
- Use complex passwords (see Introduction to Passphrases)
- Never include personally identifiable information in your passwords.

Don't Access Sensitive Information on Unprotected Devices

- Don't expect hotels and cafes to have secure wireless connections. Never access sensitive information from public computers or devices, as others could also access it.
- Malware could potentially allow onlookers to steal information like usernames, passwords, and credit card information from your unprotected devices.
- For some users, installing a VPN on your device for maximum security is a good practice.

Don't Leave Sensitive Information Lying Around

Note: fingerprint scanners are a helpful alternative to password security, but they don't eliminate the need for passwords.

- Avoid recording passwords on sticky notes or loose papers.
- Shred or destroy old documents that contain sensitive information.
- Always lock your devices before moving away from them.
    - On a Windows device, use the Windows key + L to quickly lock your computer.
    - On macOS, use Command + Control + Q to lock your machine.
    - Set smartphones to screenlock whenever they go into standby mode.
- Keep small devices like phones, hard drives, and flash drives close at hand, especially while traveling. Where possible, make use of hotel safes for these devices and laptops.

Report Suspicious Activity to our Data Security Team

- We can fix things quickly if we know about them. This keeps the issue from becoming a bigger problem.
- If you lose a device, like a smartphone or laptop, report it to us immediately. (see our Resilience Reporting Protocol here)

Introduction to Passphrases

A good password is hard to guess but easy to remember -- two factors that are often at odds with each other. Longer passwords tend to be stronger, but harder to remember.

Including numbers and symbols into a password can strengthen it while also making it harder to remember. However, often people use common substitutions, such as replacing the letter “l” with the number “1”, which are very predictable for password crackers and don't provide much additional strength. Even if a password/phrase is complicated looking, if the pattern for arriving at the pattern is simple, it may be easily guessed. The key to password strength is not obscurity, but unpredictability. Hence, some attempts to be tricky only result in a more complex-looking password which is still easy to guess.

See https://en.wikipedia.org/wiki/Passphrase for more in-depth material on passphrases and how to create strong ones.

Here are some strategies for choosing strong, memorable passwords:

Strategy 1: Use a password manager

A password manager lets you generate completely random passwords -- the strongest possible kind -- without having to memorize them. As long as you use a very strong, very memorable passphrase as your master password, this method is very secure.

- Wikipedia list of password managers

Strategy 2: Use four (or more) common words, selected at random (see this webcomic)

Surprisingly, a passphrase that consists only of un-obfuscated English words can be quite strong! The trick is that the words must be randomly selected and uncorrelated, meaning the words should not form a meaningful sentence and definitely should not be part of a common phrase. Bonus points for using uncommon words.

The trick to memorability is to find a phrase that evokes a mental image that you can remember, but that others couldn't guess.

Examples of strong passphrases

- **"correct horse battery staple"** -- common words in a non-grammatical, nonsensical configuration that still evokes an image.
- **"inside celery wiggle puppy"** -- as long as you have a way to remember this, this would also be a good random passphrase.
- **"ins1de!celerY@wiggl3#puppy"** -- obfuscating with symbols can't hurt, but it sure makes the phrase harder to remember. Remember, using symbols only provides marginal extra strength if they are predictable (as these are), so make sure the basis of the phrase is strong first.

Examples of poor passphrases

- **"Four score and seven years"** -- even though this is long (26 characters), this is a well-known quotation, and hence an awful passphrase.
- **"99 score and 24 years"** -- a little better, but even a modified quotation provides a template for an attacker to fill in random values, making it easier to guess
- **"F0ur_ScoRe_and 7 y34rs"** -- obfuscation won't help much if you use commonly used replacements on an already weak passphrase, and it only makes the passphrase much harder to remember.
- **"humongous pomegranates shimmer tantalizingly"** -- this uses four uncommon words and is actually probably pretty strong, but the words form a grammatical sentence, which significantly limits the number of guesses an attacker has to make and hence should be avoided.

Personal Security Checklist

The rest of this document has more detail on strategies for setting strong passwords / phrases, as well as a list of actions you can take to make your digital assets more secure. The items in the checklist below are divided into three priorities:

- Required for Everyone,
- Recommended, and
- Paranoid Yet Still Recommended.

Each checklist item has been assigned a hashtag[1] such as "#PS7" for "Personal Security [item number] 7" so they are easy to track and reference.

1. Set a strong passphrase/word and auto-lock on all your devices

#PS1 - Required for Everyone

Why: Even if left for a few seconds, your device could be taken and used before it locks. Setting a passphrase/word or biometric lock prevents others from using your device and accessing your

[1] These hashtags are requisition numbers in HQL for the task: meta-organizational request address-codes, or "spells".

data. Auto-lock ensures that if you leave your device unlocked and unattended (which you should never do), the maximum amount of time it can be accessed is limited.

Steps:

1. Set a strong passphrase on your desktop and laptop computers.
2. Set your computers to auto-lock after 5 minutes or less.
3. Set a strong password or biometric lock on your phone.
4. Set your phone's auto-lock feature to 3 minutes or less.
5. Repeat for any other devices you own such as tablet computers, additional phones, ebook readers, or smart mp3 players. For each device, use a distinct and unique password.

How to check the strength of a password:

1. Download this file.
    - It's the offline version of a website so it can't transmit any data.
2. Turn off your network connection (just in case).
3. Open the file in your web browser.
4. Type a password you're checking into the field and see how long it would take to crack.

2. Set a strong passphrase/word on your team chat account

#PS2 - Required for Everyone

Why: Team chat is our primary communications platform. If a team member account is compromised, it could be used to directly impersonate us.

How to change your password in team chat:

1. Open the team chat program.
2. Click the main menu (next to your user icon) and click Account Settings.
3. Click the Security tab.
4. Click the Password section to open the update password form.
5. Fill out the form with a strong new *passphrase* and click Save.
6.

3. Set strong passphrases/words on all team-based accounts you use

#PS3 - Required for Everyone

Why: Any accounts that you use for work, including both personal accounts and business accounts, could be compromised. Setting strong passphrases on every work account and every personal account you use to access work-related information reduces the chances of one and more than one account being hacked.

Steps:

1. Make a list of all business accounts, as well as personal accounts you use to access team related information, such as:
    a. Public Twitter accounts
    b. Public Facebook accounts
    c. Financial service accounts
    d. Documents-editor accounts (Workflowy, Todoist, etc.)
    e. Task management accounts (Flow, Trello, kanbans)
2. Update the passphrases on any accounts that don't already have a strong, unique passphrase set for them.

4. Set strong passphrases/words on all of the team communications channels you use

#PS4 - Required for Everyone

Why: If any of the main tools you use to communicate is compromised, a hacker could find passwords or other personal information.

Steps:

3. Make a list of all the accounts you use to communicate with regularly, such as:
    a. Email account
    b. Google account
    c. Facebook account
    d. Telegram account
    e. Reddit account
    f. Discord account
    g. Calendar account
    h. GitHub account
    i. Slack account
    j. Twitter account
4. Update the passphrases on any accounts that don't already have a strong, unique passphrase set for them.

5. Turn on two-factor authentication for all your important accounts

#PS5 - Recommended

Why: One-factor authentication (i.e. password) is not really all that secure. Two-factor authentication (2FA) adds a significant security hurdle for potential hackers. More info

Steps:

1. Enable two-factor authentication on any account that represents your identity and which someone could use to impersonate you. Some online services which support 2FA include:

    a. Google (how many Google accounts do you have). Note, 2FA should be required for your team-hosted email accounts.
    b. Facebook
    c. Twitter
    d. Online banking (almost always)
    e. Paypal
    f. Cryptocurrency accounts such as Coinbase (usually)
    g. Sprout Social
    h. Amazon?
    i. Digital Ocean
    j. LastPass
2. Perform the loopback on each account and confirm that you can still access each account.

6. Store your passwords securely

#PS6 - Recommended

Why: If you store your passwords written down in an unencrypted file or any easily-accessible place, whether physical or digital, it defeats the purpose of having secret passwords. Even storing passwords in an encrypted, hidden file is risky.

Also protip on that: if you store them in a text file label what they are for, but do not label it literally, label it contextually so that if someone got that file it would still be of little use to them: Twitter vs. "The Bird", Youtube vs. "Tubing, Mattermost vs. "Purgatory" you know whatever had context for you LOL

Steps:

1. Move your passwords to a secure method of storage.
    - An encrypted text file (try VeraCrypt)
    - An encrypted text file via command line ssl or IDE extension that invokes openssl
    - A local password manager (KeePass is open-source and can back up to DropBox)
    - A trusted password management service:
        i. LastPass (win, mac, linux, mobile, browsers)
        ii. 1Password (win, mac, linux, mobile, browsers)

How to install VeraCrypt on Linux:

Open a terminal and type these three commands.

```
sudo add-apt-repository ppa:unit193/encryption
sudo apt update
sudo apt install veracrypt
```

Note: Please use a secure password sharing service such as LastPass to share passwords with others. Don't just reveal the password to others; utilize the sharing service to maximize security. (Here's an article on how to do this with LastPass)

7. Turn off your browser's "save passwords and info" features

#PS7 - Recommended

Why: Your browser's saved passwords and auto-fill forms feature is a security nightmare. If someone sits down at your computer, they already have access to all your accounts and personal information. If you log into your web browser account on another computer, or if your web browser account is hacked, this information could also be compromised.

How to export your passwords from Chrome:

1. Navigate to "chrome://flags" in the Chrome browser.
2. Type "export" in the search box.
3. Select the dropdown box next to "Password export" and change it to Enabled.
4. Click the Relaunch Now button that appears to restart Chrome.
5. When Chrome reopens, click the main menu button, then click Settings.
6. Type "password" into the search box and then click Manage passwords.
7. Click the menu button (three dots) to the right of the words "Saved Passwords" and click Export.
8. Save the file to your hard drive (NOT a cloud drive).
9. Open the file and confirm that your passwords exported correctly.
    a. Use a plain text editor to open the file.
    b. A .csv file is "comma-separated values" and you can also open them with a spreadsheet program. (Do not use Google Sheets for this since this will put your passwords online, unencrypted.)
10. Return to chrome://flags in Chrome, search for "export" again, and disable the Password export feature.
11. Immediately, move your passwords to a secure storage method.
12. Confirm that your passwords are safely stored and accessible in the new system.
13. Delete the exported passwords file from Chrome. Shred it if you have a file-shredder (MacOS has one built-in).

How to remove your passwords from Chrome:

1. Click the main menu.
2. Click Settings.
3. Type "password" into the Settings search box.
4. Click Autofill settings.
5. Remove all the saved addresses.
6. Remove all the saved credit cards (click the  to open in a new tab).
7. Click the "On" toggle to turn Autofill Off.

8. Click the back arrow.
9. Click Manage passwords.
10. Remove every password.
    a. For password you want to save, copy them into a secure password storage place.
    b. http://www.intowindows.com/how-to-backup-saved-passwords-in-google-chrome-browser/
11. Click the toggle to turn Manage Passwords off.

How to stay signed-out of key websites you use
#PS7a - Recommended for those traveling

For those traveling with laptops, it's especially important to prevent any possibility of someone being able to steal our laptop and use our logged-in websites to access our data and impersonate us.

1. Remove passwords (at least to team-based and your primary communication channels) from your web browser's saved passwords.
2. Clear your cookies.
3. Always uncheck "stay signed-in" when you log into team-based accounts or accounts that you use for primary personal communication.

8. Clean up your cloud drives and publicly-hosted files

#PS8 - Required for Everyone

Why: If someone gains access to your team-based storage drive, they could find all kinds of personal information and work-related documents which you forgot were there.

Steps:

1. Take an inventory of the entire contents of your team storage drive.
2. Ensure all team related work documents live in the team-based drive, not your personal drives.
    a. Make sure you back up using other means!

9. Check security settings on shared work files

#PS9 - Recommended

Why: It's easy to accidentally share a file on a cloud storage drive with the entire world. Make a habit of checking the permissions of documents you use, and double-checking that they are shared correctly.

Steps:

1. Browse through the shared storage drives or your browser history to find Google Docs, Sheets, and other Drive files that you have used recently. (You access these drives by logging in here with your team-hosted email address.)
2. Check the permissions on each file. Make sure that only people who should have access to the file do!

How to remove someone from lots of files quickly in Google Drive:

1. Shift-click to multi-select documents.
2. Right-click-->sharing->advanced

10. Make sure your GitHub/GitLab SSH key includes a passphrase

#PS10 - Recommended

Using github/gitlab with SSH and having a password on SSH private keys.

Instructions

Contact Eric for help setting this up.

11. Get a cheap burner phone to receive two-factor authentication texts on

#PS11 - Paranoid Yet Still Recommended

Why: Using a simple burner phone with no apps exclusively for receiving two-factor authentication loopbacks materially secures your two-factor authentication process.

1. Get a cheap burner phone. If you're in the US $10 walmart straight talk with minutes/text on it. If you're out of the US I don't have specific instructions. Basically go to a place that sells prepaid phones, and buy the cheapest one. They are all terrible, it doesn't matter you just need it for text messages.
2. Set a password and 1-minute auto-lock on your new phone.
3. Change the phone number stored with each of your accounts that uses two-factor authentication to point to your new phone.
4. Carry your 2FA burner with you everywhere for hacker cred.

12. Put tape or webcam cover over your camera

#PS12 - Paranoid Yet Still Recommended

Why: If your computer is hacked, someone can watch you through your camera! Mark Zuckerberg puts tape on his camera—shouldn't you?

How to put tape on your camera:

1. Get some tape—NOT CLEAR.

    a. Electrical tape works well and lasts months (thanks Ferananda!).
    b. Many webcam cover products exist on the market
2. Put it on your camera.

13. Use a VPN all the time, especially on public wifi networks

#PS13 - Paranoid Yet Still Recommended

Why: Using a Virtual Private Network (VPN) means that all of your internet traffic will be encrypted and routed to another computer somewhere else in the world, before emerging into the Internet proper. This makes it harder to trace your communications to your physical location, and it also makes your identity and address more obscure in general, making it more difficult to find you online in general.

Steps:

1. Get a VPN service such as:
    a. vpn.ht (recommended by GC and Anders)
    b. mullvad or nord (recommended by Ray and Sami and David)
    c. perfect-privacy (recommended by Sami)
    d. Private Internet Access (recommended by Jamison)
2. Use your VPN service's help files to set up the VPN correctly on your computer.
3. Install or activate a script to automatically turn your VPN on all the time, and to disable internet traffic when your VPN is not connected.
    a. One way to do this is to turn off auto-connect on your wifi. Then you will always have a chance to connect your VPN when you connect to wifi.

14. Use a hardware wallet for all your cryptocurrencies

#PS14 - Recommended

Why: If anyone steals your private key, they will drain your account. A hardware wallet keeps your private key encrypted on the device, and your private key never leaves the device. It is only decrypted when you plug the hardware wallet into your computer and enter your PIN. You can back up your hardware wallet by writing down the list of keywords in a secure location (or ideally, multiple distributed loca tions or people).

Steps:

1. Get a hardware wallet such as Trezor.
2. Plug in your hardware wallet and follow it's instructions to set it up. It's pretty easy.
3. Ask trusted crypto friends if you have any questions.

Finally: Get Help

If you need assistance or advice doing anything in this document, email us at _____ (internal use only)

Report data security incidents at _____ using [this form].

When you've completed this checklist, document this on your (Trello) Onboarding checklist!