DEALING WITH PASSWORDS

E-mail, social media, file-sharing, banking, transport, entertainment ...
Nowadays, most people have dozens of accounts online - and almost all of them need passwords.
Keeping up with your own passwords can sometimes feel overwhelming.

It doesn't have to be. Here's a quick guide on how to make handling your passwords simpler.

KNOW YOUR VITALS

Not all online accounts are equal. Some are 'nice to have'; others are **CRITICAL** - losing them will seriously disrupt your life. These are usually accounts related to your **money** and your **identity**.

Focus first on the accounts vital to your life; make sure the passwords for these are top-notch. Once they're secured, move on to the less important stuff.

Banks, credit cards, loans
Accounts with direct access to your finances

Webmail
Web-mail accounts used to recover passwords for other accounts

Online shopping
Accounts that store your credit card or bank details

Reputation
Accounts identifying you, your work or affiliations

File-sharing
Accounts with documents on your finances or security

Image-sharing
Accounts with images of you or your loved ones

MAKE IT UNIQUE. MAKE IT STRONG.

Next, give your vital accounts a unique, strong password.

The easiest way to do that is to use a simple, easy-to-remember system that lets you create many passwords with little effort. Here are a couple of systems you can try (but don't use the example passwords shown here).

Or play around and build a creation system of your own. Just keep the following in mind:

8 OR MORE CHARACTERS

****

No less than 8 characters; the more the better

MIX CHARACTER TYPES

AA aa
1234 !@#$

Many sites demand a mix of uppercase, lowercase, numbers & special characters

RESET

What is your pet's name?

The answer for the password reset question should also be unique, strong - and not found anywhere online

BASE/PIN

Combine the BASE and PIN to create a unique password for a site.

The BASE **aMa229**

Identifies the site (e.g., Amazon). It's different for each site and can be written down somewhere.

Keep this secret
The PIN lolcat!

A short sequence that always stays the same. Memorize this.

Add the PIN to the front, back or even middle of the BASE:

PIN can go here...
lolcat! **aMa229** lolcat!
...or here

PHRASE PLAY

Use a phrase that's easy to remember - a song lyric, a rhyme - and use variations of it to create a password for each site.

The PHRASE
Why on earth must I create so many passwords

Then play around variations of the phrase for each site. You can try:

whyonearthmustI
Using it as is.

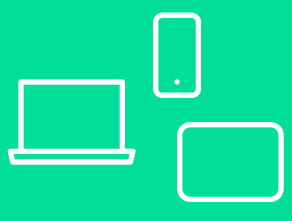
woemIcsmp
Making an acronym.

2|hoerhutceeoasod
Using every second character.

You can also include a BASE with these

JUST GENERATE IT

There are many programs, apps and even scripts that can save you the headache and generate a strong, unique password for your accounts. Give them a try.



Make sure the result is unique and strong

NOT THESE

The worst kind of password is one that everyone else uses. According to news reports on major database breaches in 2013 [1], these are some of the most common passwords people use.

- ✗ password
- ✗ passw0rd
- ✗ password1
- ✗ qwerty
- ✗ abc123
- ✗ aaaaaa
- ✗ admin
- ✗ master
- ✗ iloveyou
- ✗ letmein
- ✗ work
- ✗ job
- ✗ shadow
- ✗ princess
- ✗ 1234
- ✗ 12345
- ✗ 123456
- ✗ 1234567
- ✗ 12345678
- ✗ 123456789
- ✗ 1234567890
- ✗ 000000
- ✗ 111111
- ✗ 123123
- ✗ 654321

These are not strong passwords. **Don't use these.**

2FA IF THEY HAVE IT, USE IT

Don't depend on passwords alone. Many major online services now offer an additional security feature - **2-Factor Authentication (2FA)** [2]. If it's available, enable 2FA on your vital accounts so that even if someone steals your password, they still only have half of the 'key' needed to get into your account.

These are just some of the services that offer 2FA:

FACEBOOK **PAYPAL** **APPLE** **TWITTER** **GOOGLE** **EVERNOTE** **WORDPRESS** **MICROSOFT** **LINKEDIN** **DROPBOX** **YOUNITED** **ETSY**

SAVE IT SAFELY

Once you have your passwords, keep them safe from prying eyes. Some people write them down on paper and lock it away in a safe place. Others keep them in an encrypted file on a device. Still others use a password manager. Find a way that's **safe and easy** for you.

Keep the passwords safe

[1] BBC; *Analysis reveals popular Adobe passwords*; 5 Nov 2013; http://www.bbc.com/news/technology-24821528

[2] Seth Rosenblatt; CNET; Two-factor authentication: What you need to know (FAQ) ; 23 May 2013; http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

How F-Secure can help you?

KEY
Our secure password manager F-Secure KEY has a password generator, so that you can create stronger and safer passwords to all your online accounts.

Moreover, you don't need to remember those passwords! You only need to remember one master password to access them all, and KEY works on all your devices so you always have your passwords with you on the go.

Download KEY for free: **f-secure.com/key**

For more info about passwords and keeping your data safe, visit:
www.f-secure.com/labs/passwords

For more articles about information security, visit:
www.f-secure.com/labs

F-Secure