

# Password Security and Management – The Essentials

Denise Wassenaar

October 4, 2023





# Introduction

About me  
Why this class?

# SMISHING PHISHING

**Before we get to Passwords**

# Phishing

---

Scammers use email to attempt to trick you in responding.

Then, they try to steal your passwords, account numbers, or Social Security numbers.

---

If they get that information, they could get access to your email, bank, or other accounts.

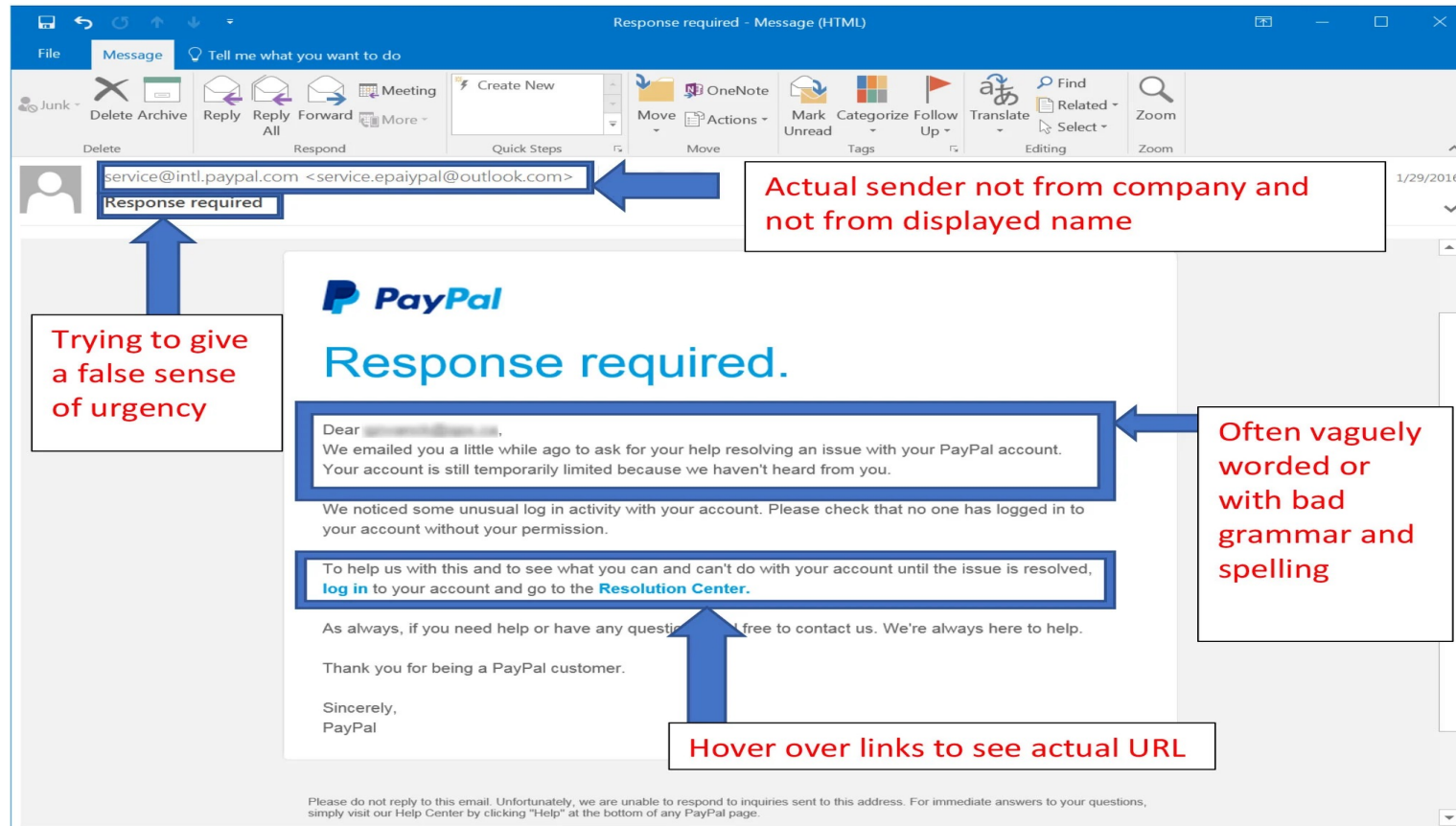
---

Or they could sell your information to other scammers.





# Anatomy of a Phishing Email



Even if you think the email is legitimate, if it is not something you are expecting it is a good idea to contact a person you believe to be the sender “out-of-band,” or by another method than clicking “reply” or any link in the email. For example, call a phone number you know belongs to the institution or person or go directly to their website by typing in the URL.

\*original image taken from [phishing.org](http://phishing.org)

# FedEx®

## Express

### Parcel Tracking

Dear Customer,  
There is a package bearing your name at our local dispatch facility.  
Our courier was unable to deliver the parcel due to incorrect delivery d  
Please see below to confirm your delivery address with us to ensure sm

[FedEx Parcel Tracking Info](#)

Best Regards  
FedEx Redstar Express



## Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

**REF CODE:2550CGE**

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

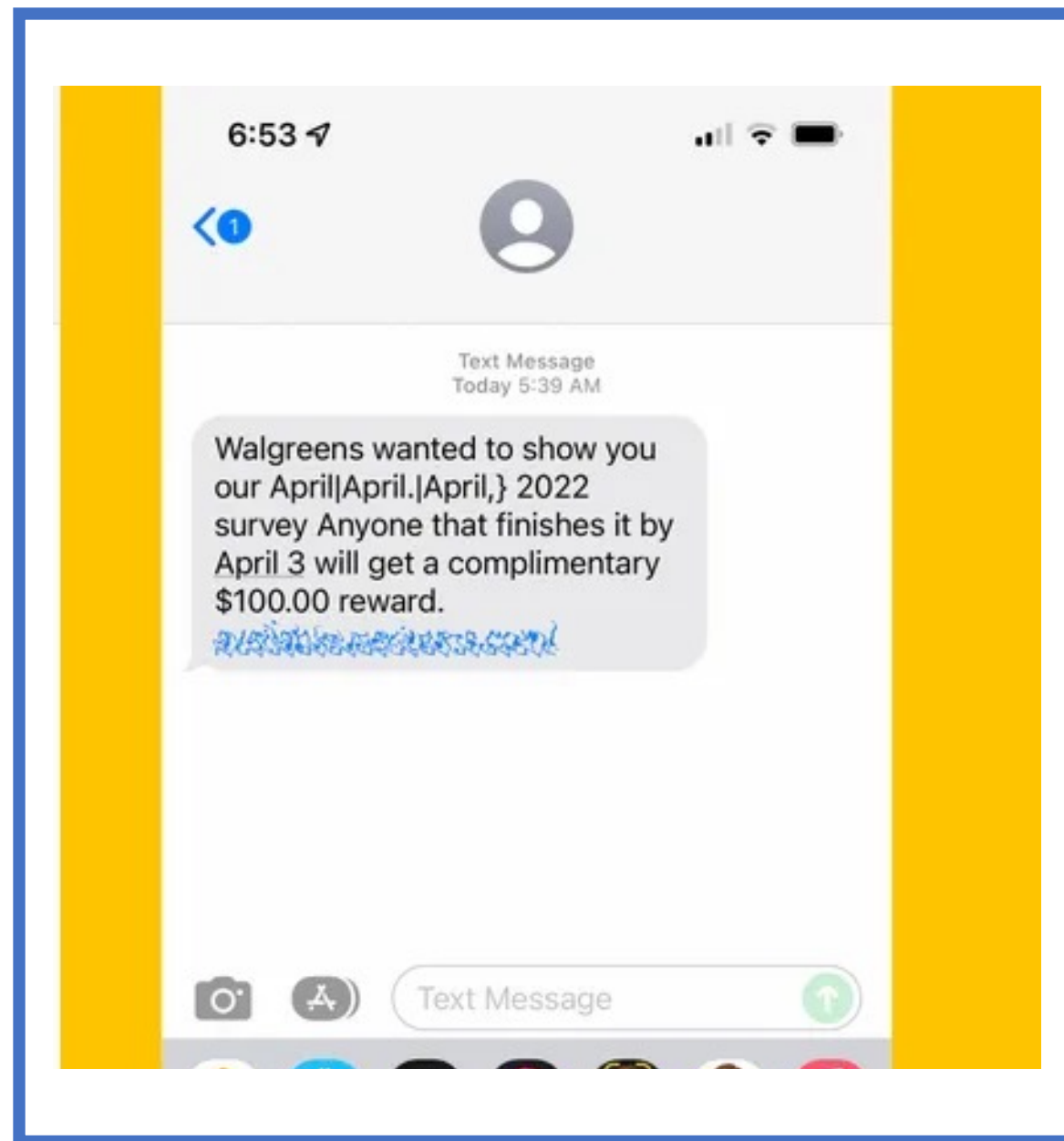
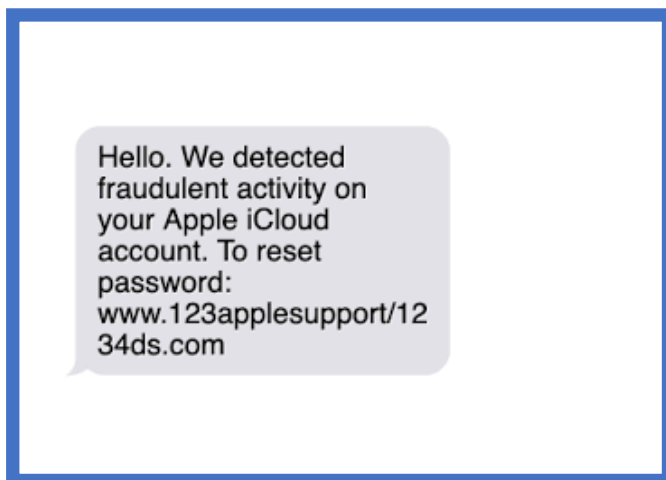
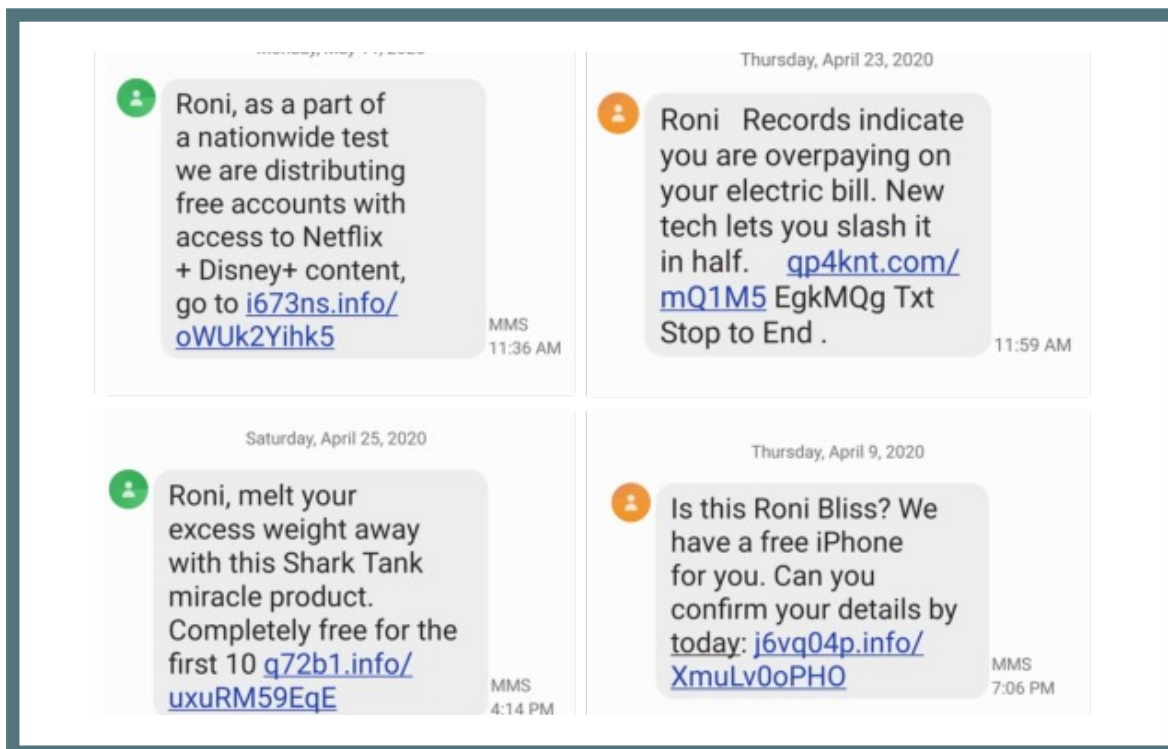
[Amazon.com](#)

Email ID: 

# Smishing

- A type of phishing occurs via your text messages
  - Texts from banks, investment firms and other financial institutions stating there's an issue with your account.
  - Messages promising free money, products or services.
  - Text messages from companies & service providers stating that there's an issue and you need to update your payment account information.





# Today's Discussion

---

Discuss why password security is essential

---

Learn tips for creating strong passwords

---

Comparison of popular password management systems







Why password security  
is essential.

---

Question:  
Do you  
mostly ...



Connect with other people?



Bank and shop?



Watch movies and play games?



What else do you do?



# Password Security

- People are in the business of stealing data and account information.
  - First half of 2020 alone, over 36 billion records were part of a data breach.
  - There is a hacking attempt somewhere in the US every 39 seconds.
- Your passwords are the padlock that protects your livelihood, money, and identity.
- It's dangerous to *assume* that the password we are using is strong and that it is *good enough*.



Why is password security important?

---

# Password Threats

- THREATS
  - **You** (Too trusting and don't believe it will happen to you)
  - Easier to guess than expected
  - Brute Force
  - Use familiar tricks
    - Transformation and substitutions (f00tb@ll)
    - Keyboard patterns (qwertyasdf)
    - Padding (Montana12&\*-&\*-&\*-&\*)

# The Most Common Poor Password Practices

Create easy passwords

Reuse passwords

Never changing passwords

Sharing passwords insecurely

Writing passwords down or storing them on spreadsheets or your phone

Use the minimum length passwords

# List of the 20 passwords commonly found in leaked information on the dark web:

23456  
123456789  
Qwerty  
Password  
12345  
12345678  
111111  
1234567  
123123  
Qwerty123



1q2w3e  
1234567890  
DEFAULT  
0  
Abc123  
654321  
123321  
Qwertyuiop  
Iloveyou  
666666

# Data Breach Defined

---

An incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

---

A small company or large organization may suffer a data breach.

---

Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, passwords, trade secrets, or matters of national security.

# Data Breaches in 2023

---



## Top 9 High-Profile Company Data Breaches in 2023

- T-Mobile: May 2023 (and January 2023)
- Yum! Brands (KFC, Taco Bell, & Pizza Hut): April 2023.
- ChatGPT: March 2023.
- Chick-fil-A: March 2023.
- Activision: February 2023.
- Google Fi: February 2023.
- MailChimp: January 2023.
- Norton Life Lock: January 2023.



# How a hacker works

Hackers start with a bunch of wordlists. The top 10,000 passwords is a good place to start. Also, lists of all English words, all names, dates, and so on. In less than one second, 30% of all passwords will be cracked.

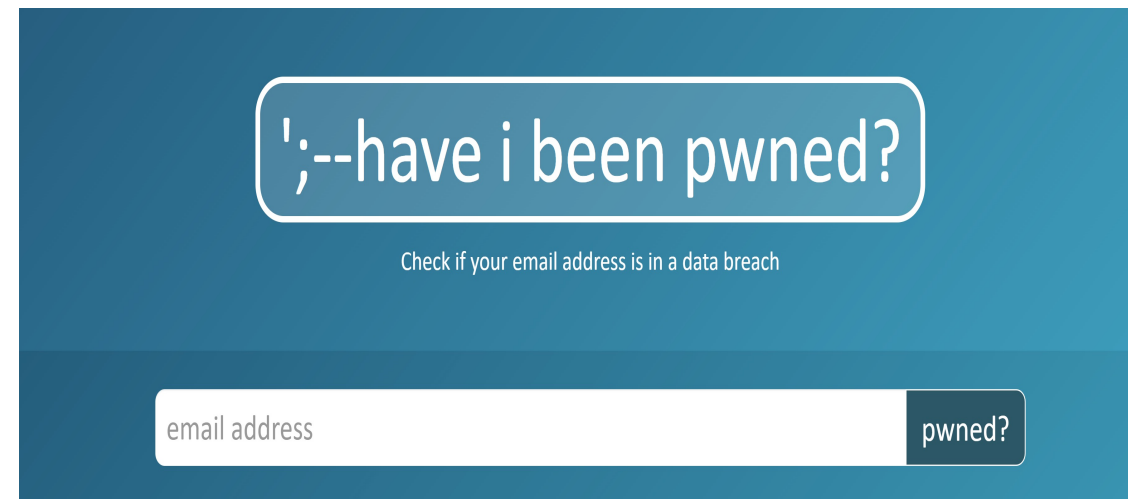
After exhausting those wordlists, they will try all of the words again with common substitutions: capitalizing the first letter (december → December), making common letter-for-number swaps (december → d3cemb3r), and other common password variations.

Next, they start combining the previous wordlists. Name + date (doug3251983). Name + [separator] + date (doug.3251983).


If all else fails: brute force, a.k.a. try every combination of characters. Try a, then b, then c ... eventually aa, ab, ac ... eventually 6j2b#hi8, 6j2b#hi9, 6j2b#hi0, et cetera.

# Have I Been Pwned?

- I got **pwned**,” which **means** that hackers stole personal details.
- <https://haveibeenpwned.com/>



The image shows a screenshot of the 'Have I Been Pwned?' website. The background is a solid blue color. At the top, there is a white rounded rectangle containing the text 'have i been pwned?' in a lowercase, sans-serif font. Below this, in smaller white text, is the phrase 'Check if your email address is in a data breach'. At the bottom of the interface, there is a white input field with the placeholder text 'email address' and a dark blue button to its right with the text 'pwned?' in white.



# Learn tips for creating strong passwords

Objective 2

# How to make a strong Password

! " # \$ % & ' ( ) \* + , - . / :  
; < = > ? [ \ ] ^ \_ ` { | } ~



- At least 12+ characters long (the longer, the better).
- Has a combination of:
  - Uppercase letters A-Z
  - Lowercase letters a-z
  - Numbers 0-9
  - Special Symbols ~`! @#\$%^&\*()\_ - +={[]|\:;'"<, > . ? /
- Random and unique.

# Multi-Factor Authentication (MFA)

- A factor in authentication is a way of confirming your identity when you try to sign in.
- The three most common kinds of factors are:
  - Something you know - A password or a memorized PIN.
  - Something you have – A smartphone (phone number) or a secure USB key.
  - Something you are - A fingerprint or facial recognition.

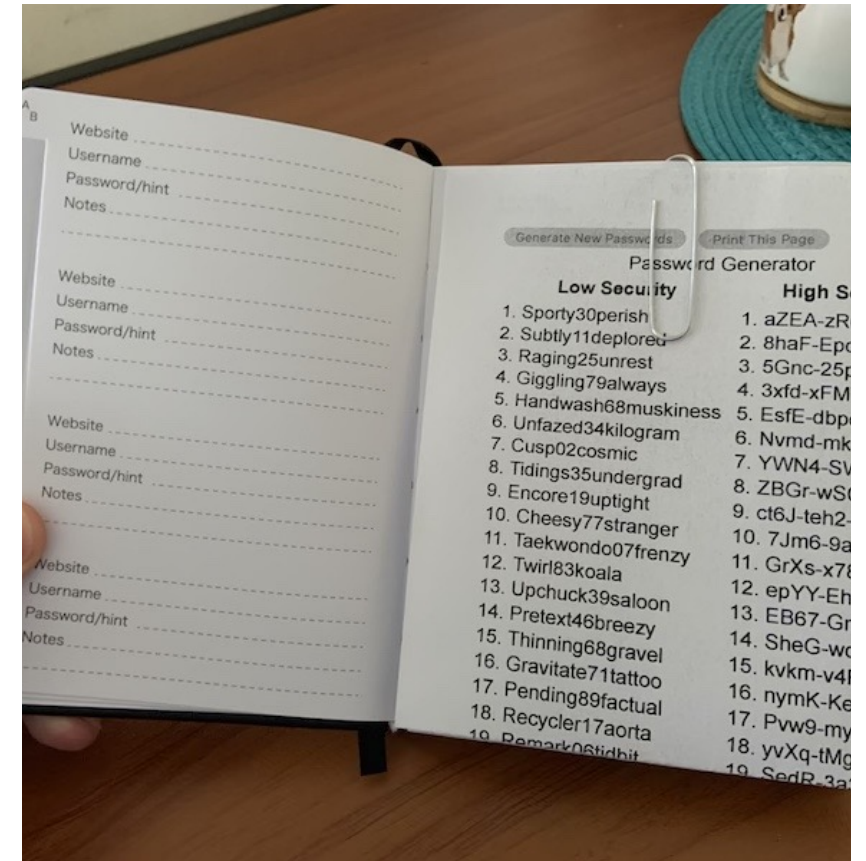




Jo Heller  
©2014 HELLER.com

# How To Make Unique Passwords

- An easy-to-make unique password – Use a password generator
  - <https://passwordbits.com/password-gen.html>
- **Low-security** passwords:
  - For non-important accounts:
    - Netflix, forums, or any account that would be a mild inconvenience if hacked.
- **High-security** passwords:
  - For essential accounts:
    - Banking and email, or anything you would panic over if it were hacked.






# TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



# Password Checkers

- Password:
    - *You can actually use spaces in your password!*
  - NordPass
    - <https://nordpass.com/secure-password/>
  - Kaspersky
    - <https://password.kaspersky.com/>
  - All Things Secured
    - <https://www.allthingssecured.com/password-checker/>
- 

The word "QUESTIONS" is written in a large, white, bold, sans-serif font with a slight 3D effect. It is centered horizontally and surrounded by a cluster of overlapping squares in various shades of blue and green. The squares vary in size and opacity, creating a dynamic, abstract background for the text.

QUESTIONS



# Comparison of popular password management systems

Objective 4

# Ways People Keep their Passwords

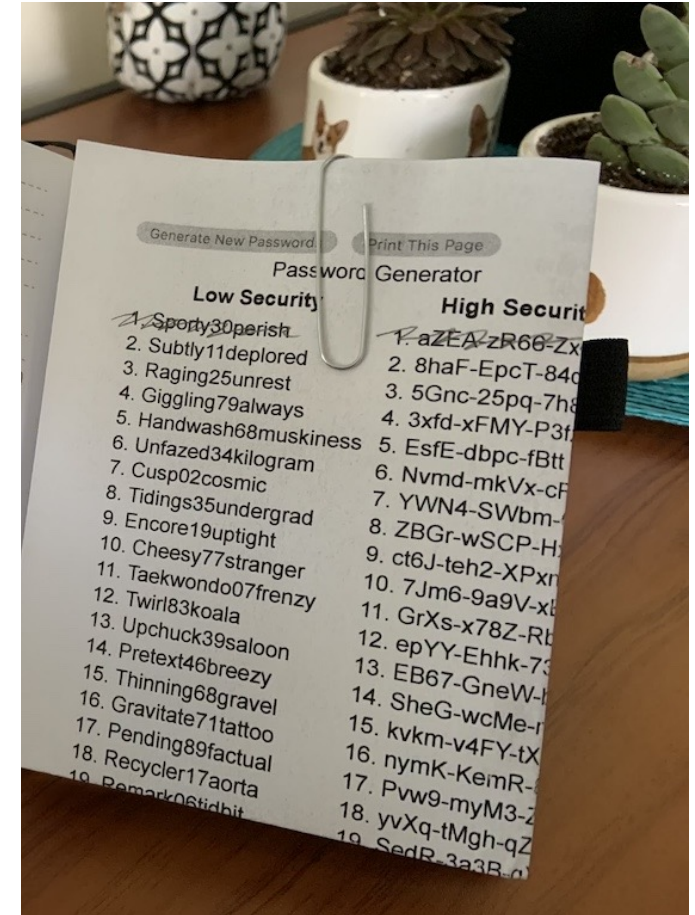


- Post-It Notes
- Taped to the bottom of their computer or keyboard
- Text, Word, and Excel file on their desktop (password protected or not)
- No place; they use (one, two, or three) main passwords and rotate between them



# Paper and Pencil

- Putting a “dot” under the capitalized letters helps you remember that they are capitalized.
- It’s also smart to use a pencil instead of a pen in case you make a mistake or need to change the password later.
- [https://www.amazon.com/s?k=password+book+for+senior&rh=n%3A1064954%2Cp\\_72%3A1248945011&dc&ds=v1%3AaxqyTfLeOf2mkPVjSOQ6vTvyftxXG3oW%2F%2FCEY3bKE%2BPU&qid=1671209459&rnid=1248943011&ref=sr\\_nr\\_p\\_72\\_1](https://www.amazon.com/s?k=password+book+for+senior&rh=n%3A1064954%2Cp_72%3A1248945011&dc&ds=v1%3AaxqyTfLeOf2mkPVjSOQ6vTvyftxXG3oW%2F%2FCEY3bKE%2BPU&qid=1671209459&rnid=1248943011&ref=sr_nr_p_72_1)



# Password Management Strategy

## Critical passwords you must know.

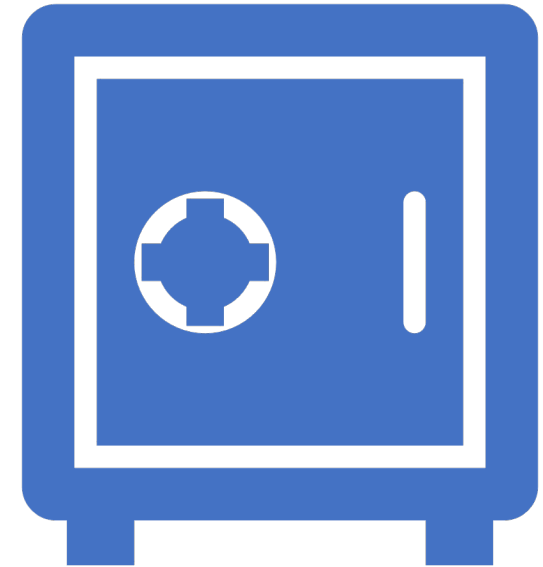
- Ones you use often or in emergency access to everything else.
- Common Examples:
  - Master password for a password manager
  - Computer login password
  - Your Apple ID password
  - Dropbox or cloud storage password
- Create solid but memorable passwords for these
- Practice and memorize them

Use a password manager for everything else



# Password Managers

- A software vault that stores your passwords encrypted.
- Has a master password that grants access to all the other passwords
- Can generate and store random complex passwords that you can use instead of less complex passwords.
- Syncs your passwords and makes them available on the devices you use, wherever you are, even without internet access.



# Suggested Features

---

Works in a browser, phone, and tablet.

---

Autofills most places (occasionally, you'll need to cut and paste)

---

Syncs via Dropbox, iCloud, or their cloud service

---

Preferably syncs automatically, not just when you manually initiate

---

Allows you to share specific logins securely with other people (like family members)

# Apple's iCloud Keychain

- Pros:
  - Great for **remembering passwords on web pages** and storing those details,
  - Visit a website it will automatically display the username and fill the password in for you, at least if you have set it up in Safari Preferences.
- CONS:
  - Becomes useless when trying to access anything other than websites
  - Not recommended if you need to sync your passwords and credit cards, app logins, identities, banking credentials, and much more across all your devices





# What is a Browser-based Password Manager

Google Chrome, Edge, Firefox, Opera, Safari, and Brave enable in-browser password management by default.

Similar to standalone alternatives in terms of basic function.

---

# Web based Password Manager and Generator

---

## **ADVANTAGES**

**Very convenient and user-friendly.**

---

**Useful password generator feature.**

---

**Passwords are synchronized across all devices.**

---

**No payment required.**

---

# Web based Password Manager and Generator

---

## DISADVANTAGES

**Only relatively safe.**

---

**No cross-browser syncing of passwords.**

---

**Limited security features and functionality.**

---

**Comes with a lot of risk.**

---

If you use Chrome and your Google account is successfully attacked by hackers, for example, all of your data may be readily available to them.

---

# Example Password Managers












- 1Password – <https://1password.com/>
- Dashlane – [www.dashlane.com](http://www.dashlane.com)
- Roboform – <https://www.roboform.com/>
- Keeper – <https://www.keepersecurity.com/>

**The only acceptable Free manager:**

- Bitwarden - <https://bitwarden.com/>



	 Lastpass	 KeePass	 1Password	 Dashlane	 Passwordstate	 Keeper	 Sticky Password	 Devolutions Password Server	 RoboForm
Offline Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Browser Integration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Autofill Forms	✓	✗	✓	✓	✓	✓	✓	✓	✓
Password Generator	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Alert	✓	✗	✓	✓	✗	✗	✗	✓	✗
Portable Application	✓	✓	✗	✓	✗	✓	✓	✗	✓
Mobile Application	✓	✓	✓	✓	✓	✓	✓	✗	✓
Security Audits	✓	✗	✓	✓	✓	✓	✗	✓	✓
Import Passwords	✓	✓	✓	✓	✓	✓	✓	✓	✓
Export Password	✓	✓	✓	✓	✓	✓	✓	✓	✓
Single Sign-On (SSO)	✓	✗	✗	✗	✗	✓	✗	✓	✓
Password Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrated Database	✓	✗	✓	✓	✓	✓	✓	✓	✓
On-Premise	✗	✓	✓	✗	✓	✓	✗	✓	✗
Cloud Based	✓	✗	✓	✓	✗	✓	✓	✗	✓

	Built in		
	Chrome	Edge	Keychain (Safari)
Generates passwords for you	✓	✗	✓
Verifies that site isn't impostor	✓	✓	✓
Identifies re-used passwords	✗	✗	✓
Blinded to customer support	✗	✗	✓
Recovery via physical object	✓	✓	✗
Recovery via trustee	✗	✗	✗
Published security architecture	✗	✗	✗

The word "QUESTIONS" is written in a large, white, bold, sans-serif font with a slight 3D effect. It is centered horizontally and surrounded by a cluster of overlapping squares in various shades of blue and green. The squares vary in size and opacity, creating a dynamic, abstract background for the text.

QUESTIONS

*The  
End*