

Passwords, Managers, and Other Stuff

password***



Helps to stay safe on your computer

Score	Description
Less than -50	Um. I'm not even sure why you pretend you are using passwords.
-50 to 0	Please reconsider your password habits – they are probably giving you a false sense of security.
0 to +15	In general, your password practices are not unreasonable. Check the quiz again to see how much more paranoid you are willing to get.
+15 and up	Greetings fellow paranoid security geek. Nice to know someone takes this seriously.

PASSWORD AS DEFINED BY

A password is a basic security mechanism that consists of a secret pass phrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination.


A password is used to restrict access to a system, application or service to only those users who have memorized or stored and/or are authorized to use it.

A password may also be called an access code, PIN or secret code

Securing your system with passwords and pin codes could prevent kids and computer-inexperience people from gaining unauthorized access to your system (any system, ranging from mobile phones, laptop computers, etc.), but it will only slow down a hacker.

KINDS OF PASSWORDS.

Weak Passwords

- ▶ based on common dictionary words
 - ▶ Including dictionary words that have been altered:
 - ▶ Reversed, Mixed Case, Character/Symbol Replacement
 - ▶ based on common names
 - ▶ short (under 6 characters)
 - ▶ based on keyboard patterns (e.g., “qwerty”)
 - ▶ composed of single symbol type (e.g., all characters)
 - ▶ are difficult for you to remember
- 

KINDS OF PASSWORDS.

Strong Passwords

- ▶ Contain at least *one of each* of the following:
 - ▶ digit (0..9), letter (a..Z), punctuation symbol (e.g., !), control character (e.g., ^s, Ctrl-s)
- ▶ Are based on a verse (e.g., passphrase) from an obscure work where the password is formed from the characters in the verse
 - ▶ e.g., “W0tstwtwoO” derived from the song,
 - ▶ “Were off to see the wizard the wonderful wizard of Oz”
- ▶ Use a password checker (passwordchecker.com).
- ▶ Don't save passwords in a browser.
- ▶ Use a password manager.

6 COMMON PASSWORD MISTAKES PEOPLE MAKE

- ▶ **Same password, different site:** 38% have once reused the same password on two different services, the study says.
- ▶ **Password tweaking:** 21% have once modified an existing password to sign up for a new service (52% have reused the same password or tweaked one, collectively).
- ▶ **'Password Walking':** Researchers discovered a high number of passwords using letters and numbers adjacent to each other, a practice known as "password walking" ("qwerty" is an example).
- ▶ **Love & #\$%#@:** The study says it found a large number of passwords using the word "love" or an expletive. Either way, it's not secure.
- ▶ **Pop culture terms:** "superman" was the #1 superhero-related password. "pokemon" was #2 and "star wars" and "spiderman" made the top 10.
- ▶ **Sports teams:** Sure we all love our hometown teams, but that's making it too easy for the hackers, according to the study. Perennial Champions League football clubs such as Liverpool and Manchester turned up often in the results.

The Top 25 Worst Passwords of 2019

- | | | |
|---------------------------------------|------------------------|----------------------------|
| 1 - 123456 (rank unchanged from 2018) | 11 - abc123 (Up 4) | 21 - 888888 (New) |
| 2 - 123456789 (up 1) | 12 - qwerty123 (Up 13) | 22 - princess (Down 11) |
| 3 - qwerty (Up 6) | 13 - 1q2w3e4r (New) | 23 - dragon (New) |
| 4 - password (Down 2) | 14 - admin (Down 2) | 24 - password1 (Unchanged) |
| 5 - 1234567 (Up 2) | 15 - qwertyuiop (New) | 25 - 123qwe (New) |
| 6 - 12345678 (Down 2) | 16 - 654321 (Up 3) | |
| 7 - 12345 (Down 2) | 17 - 555555 (New) | |
| 8 - iloveyou (Up 2) | 18 - lovely (New) | |
| 9 - 111111 (Down 3) | 19 - 7777777 (New) | |
| 10 - 123123 (Up 7) | 20 - welcome (Down 7) | |

IF YOUR PASSWORD IS ON THIS LIST, IT'S TIME TO CHANGE IT !

WHAT IS PASSWORD MANAGERS

A password manager is a software application or a hardware device used to store and manage a person's passwords and strong passwords. Typically all stored passwords are encrypted, requiring the user to create a master password to access all the stored, managed passwords.

onelogin




1Password

dashlane

LastPass...

 RoboForm

WHY USE A PASSWORD MANAGER

- ▶ To take a load off your mind.
 - ▶ To avoid password reuse.
 - ▶ Strong unique passwords for every account / website.
 - ▶ Only need to remember one master password
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.


WHAT TO LOOK FOR IN A PASSWORD MANAGER

- ▶ Password Generation
 - ▶ Autofill and Auto–login
 - ▶ Secure Sharing
 - ▶ Two-Factor Authentication
 - ▶ Protection for other personal data
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against the blue background.

DEMO



6 STEPS TO SECURE WINDOWS 10

- ▶ **Create a Restore Point**
 - ▶ **Get Rid of Bloatware**
 - ▶ **Install Updates**
 - ▶ **Local Accounts Only**
 - ▶ **Shut Down Stalkerware**
 - ▶ **Enable Firewall and A/V**
- 

ACCOUNT TYPES

▶ Microsoft Account

- ▶ Default in Windows 8 and later; user can install programs and make system changes; they sign in with their Microsoft password, and the account is synced with the Microsoft Store.

▶ Administrator

- ▶ The administrator controls the entire computer, deciding who gets to play with it and what each user may do on it. On a computer running Windows, the owner usually holds the almighty Administrator account. He or she then sets up accounts for each household member and decides what they can and can't do with the PC.

▶ Standard User

- ▶ Standard account holders can access most of the computer, but they can't make any big changes to it. They can't run or install new programs, for example, but they can run existing programs.

▶ Child

- ▶ The Child account setting is actually just a Standard account with the Family Safety settings automatically turned on.

ADMINISTRATOR ACCOUNT

- ▶ Complete control over the OS and their apps.
- ▶ Unrestricted access to the computer.
- ▶ An exploit can more easily gain control of your system.
- ▶ It can install
rootkits, keyloggers, and other suspect services.

A malicious program that can also modify and delete files, and even prevent devices from booting.

However, using a user account with fewer privileges can block most attacks.

MICROSOFT ACCOUNT VS LOCAL ACCOUNT

▶ Microsoft Account:

- ▶ You can use the Windows Store and install apps.
- ▶ All apps automatically sign into your Microsoft Account, and will not prompt for your credentials.

▶ Local Account:

- ▶ Secure.
- ▶ Is more private.
- ▶ Always works, regardless of Internet connectivity.
- ▶ Can have any name/screen name you wish, instead of sharing your email address to everyone who walks by your locked computer.
- ▶ Can have any password you wish, and it is totally separate from your (hopefully) secure email password.

BOTTOM LINE:

- If you're not planning on using the Windows Store or any of the apps, avoid a Microsoft Account at all costs.
- Use a standard user account always
 - Apps can be installed, you will get a UAC box asking for an Administrator user name and password.

2FA (TWO FACTOR AUTHENTICATION)

- ▶ 2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are.
- ▶ This second factor could come from one of the following categories:
 - ▶ Something you know. - Something you have. - Something you are:.

VPN'S (VIRTUAL PRIVATE NETWORKS)

- ▶ allows you to create a *secure connection* to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more.
- ▶ Protect yourself from snooping on untrustworthy Wi-Fi hotspots.
- ▶ Gain at least some anonymity online by hiding your true location.

RFID ENABLED CREDIT CARDS

- ▶ Just because it has a chip doesn't mean it has RFID.
- ▶ Check for the following trade name:
 - ▶ *AMEX ExpressPay, MasterCard PayPass, VISA PayWave or Discover Zip.*
- ▶ Look for the pie-shaped logo for RFID capability



5 WAYS TO KEEP YOUR INFORMATION SAFER FROM HACKERS

- ▶ Pay attention to your passwords
 - ▶ Keep your information private when using public Wi-Fi
 - ▶ Surf safely
 - ▶ Be smart with social media
 - ▶ Keep your email secure
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against the blue background.

BASIC STREET SMARTS IN CYBERSPACE

In real life, most of us shy away from rough neighborhoods.

We lock our cars and install security systems in our houses. But we're strangely lax when we're online.

- ▶ Use a security code for your smartphone or tablet and a password for your computer.
- ▶ Don't send personal or financial information via email.
- ▶ Don't click on links you didn't expect in pop-up windows or what could be phishing emails.
- ▶ Don't share your password or username.
- ▶ Keep current with the latest software updates which are often released to patch some holes.