DANGER

Password Reuse Puts EVERYONE at RISK!

How many people reuse passwords?

65% of people **reuse passwords** across **multiple** if not all sites

Google

72% of people **reuse passwords** in their **personal life**

Hypr

The **average person reuses each password** as many as **14 times**

LastPass

76% of **millennials recycle** their **passwords**

Security.org

Nearly half (49%) of employees **ineffectively change or add a digit or character** to their password when updating their company password every 90 days.

In 2020, a staggering **44 million accounts** were **VULNERABLE** to account takeover due to the use of **compromised or stolen passwords.**

This risk impacts both personal and work accounts. **73% of all users DUPLICATE THEIR PASSWORDS** in their personal & work accounts.

Microsoft

So what? What's the risk?

Bad actors prey upon the vulnerabilities caused by password reuse. Compromised credentials and passwords are responsible for

81% of **HACKING-RELATED BREACHES.**

Verizon Data Breach Investigations Report

If **ONE Account** is compromised, **ALL Accounts** that share the password are compromised.

Hackers will **use passwords** from one site **to gain access to your banking and email** accounts.

A **compromised email** lets hackers do **password resets** and **obtain MFA** codes for other sites OR **target friends family, co-workers** with malware or phishing attacks.

Password TIPS to Keep You SAFE!

1. Use strong, unique passwords for every account.

That way, even if your password for one website is compromised, the others stay secure. This is especially crucial when you create accounts for websites that store sensitive or financial data. The graphic below shows how we've been trained to use passwords that are hard for humans to remember but easy for computers to crack. So, how do you create a strong password?

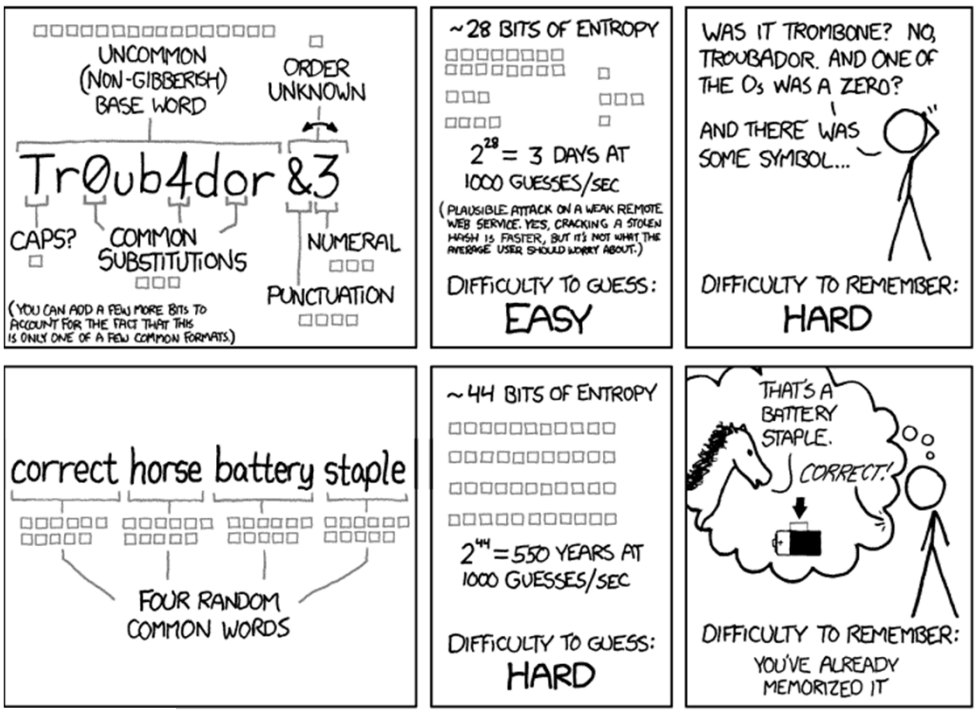
a. **Never Reuse a Password.** We've already demonstrated the danger of this. Also, when having to change a password, don't just change one character or digit.

b. **Use PassPHRASES vs. PassWORDS.** The most secure passwords are longer and harder for us to remember. PassPHRASES string together sentence-like words that are easy to remember and hard to hack. Song lyrics or verses that have significance to you or the first letters in your favorite book are great options. Even though they're longer, they're easier to recall because they relate to something meaningful to you.

c. **Include Numbers & Special Characters.** A way to incorporate numbers into your passwords is to use mathematical expressions or dates.

d. **Avoid the Obvious.** Stay away from using personal information like birthdates, pet names or family names. Avoid using common words or single words with added numbers at the end as these are super easy to breach.

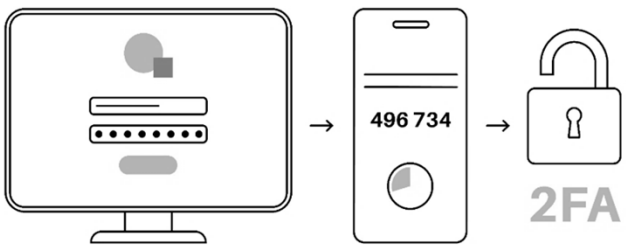
e. **Use Password Generators like KeePass, NordPass or Dashlane.** These programs automatically generate strong unique passwords for every login. But you only have to remember ONE to access the program.



SOURCE: xkcd.com

2. Never overlap work and personal passwords.

3. Turn on Multi- or Two-Factor Authentication (MFA or 2FA)



4. Protect yourself at work and home!

Safeguard your personal life too, and keep family, friends, and coworkers safe. Remember: It only takes 1 weak link.

We're Here to Help!

Pierz 320.468.6422
Sauk Rapids 320.252.5121
Eden Valley 320.453.2000
Online/Mobile FMPierz.com

CustomerService@FMPierz.com