



PASSWORD ESSENTIALS

STRONG PASSWORDS. SMART HABITS. SAFE ACCOUNTS.

Simple steps to protect your accounts, your information, and your peace of mind.



RGE TIP: Your password is the key to your digital life. Protect it like you would your house keys or your wallet.
Strong habits today prevent big problems tomorrow.



MAC NOTE: These same password best practices apply on a Mac, iPhone and iPad. Use Keychain Access and iCloud Keychain to securely store and sync your passwords.



1. EVERYONE USES THESE (ESSENTIALS • Everyday Tasks)



Use Strong Passwords

Make passwords at least 12–16 characters long. Use a mix of letters, numbers, and symbols.



Use a Different Password for Each Account

If one account is hacked, the others stay protected.



Enable 2-Step Verification (2FA)

Add an extra layer of security whenever it's available.



Never Share Your Passwords

Legitimate companies will never ask for your password.



Be Aware of Phishing Scams

Don't click links or open attachments in suspicious emails or texts.



Keep a Secure Record

Keep a written list of important passwords in a safe place (not on your computer).



Log Out on Shared Computers

Always sign out when you're finished, especially on public or shared devices.



RGE TIP: If you wouldn't say it out loud in a crowded room, it's probably too easy to guess.



2. USEFUL SKILLS (GOOD TO KNOW • Do More)



Use a Password Manager

Tools like Bitwarden, 1Password, or Microsoft Authenticator can create, store, and fill passwords securely.



Update Weak or Old Passwords

Change passwords for important accounts at least once a year.



Sync Across Devices

Let your password manager safely sync across your computer, phone and tablet.



Use Passkeys When Available

Passkeys are easier to use and more secure than passwords.



Check for Breaches

Visit haveibeenpwned.com to see if your email has been in a data breach.



Set Up Account Recovery

Add a recovery email and phone number so you can get back in if needed.



Use Secure Challenge Answers

Avoid answers that are easy to guess or find online.



RGE TIP: A password manager remembers your passwords so you don't have to.



3. ADVANCED TOPICS (USE WITH CAUTION • Control)



Understand 2FA Options

Use authenticator apps, security keys, or trusted device notifications instead of SMS when possible.



Review Active Sessions

Check where you're signed in and remove devices or sessions you don't recognize.



Watch for Unusual Activity

Look for login alerts and address anything suspicious immediately.



Use Temporary Passwords

Create unique temporary passwords for trials, guests, or short-term use.



Avoid Common Mistakes

Don't reuse passwords, write them on sticky notes, or store them in plain text files.



Backup Your Password Data

Make sure your password manager is backed up or has recovery options in case of device loss.



Extra Caution for Sensitive Accounts

Use your strongest passwords and 2FA for banking, email, health, and financial accounts.



RGE TIP: Strong security is not about one perfect password—it's about many good habits.

HOW TO GET STARTED



Review your most important accounts.



Create strong, unique passwords.



Turn on 2-step verification where available.



Use a password manager to keep everything safe.



You're more secure!

IMPORTANT SAFETY REMINDERS

- ✓ No one from a legitimate company will ask for your password.
- ✓ Beware of emails or texts that create urgency or fear.
- ✓ Use strong passwords and 2FA for your most important accounts.
- ✓ If something doesn't look right, stop and ask.



RGE GOLDEN RULE

Make your password hard to guess, and your habits easy to follow.
Strong passwords + smart habits = peace of mind.



RGE PHILOSOPHY

Teacher first.
Technician second.
People always.