Improving your Online Security

Dave Selkowitz 10/12/2023

It’s okay to worry about security because…

Why improve your online security?

- Safeguard against fraud and protect your personal information and finances
- If done correctly, security improvements can enhance your online experience
- Peace of mind

Key areas to address

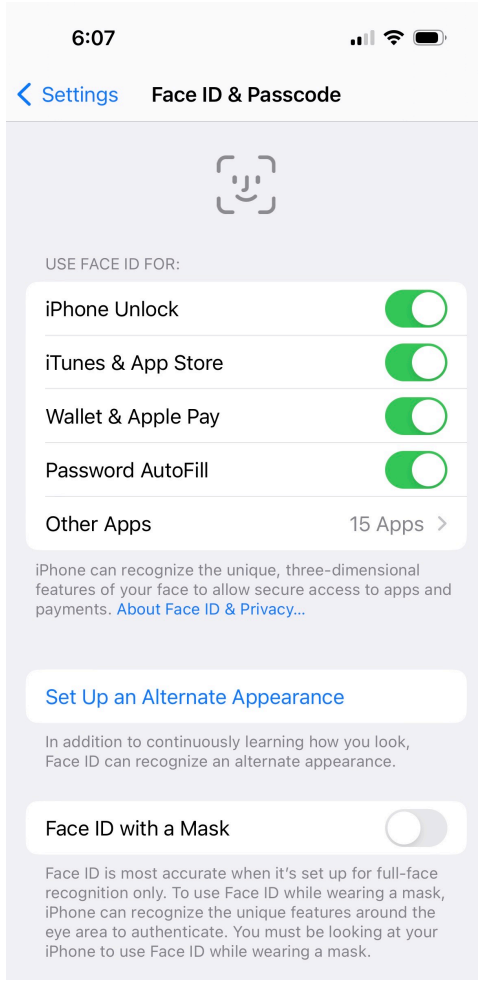
- Securing your devices - phone, tablet and computer
- Improving account security and using a password manager
- Setting up email to protect your privacy
- Using passkeys to protect critical accounts (advanced topic)


¡PHONE SECURITY? I CAN'T EVEN FIND THE DAMN THING!
CAGLECARTOONS.COM
©2016 BOB ENGLEHART

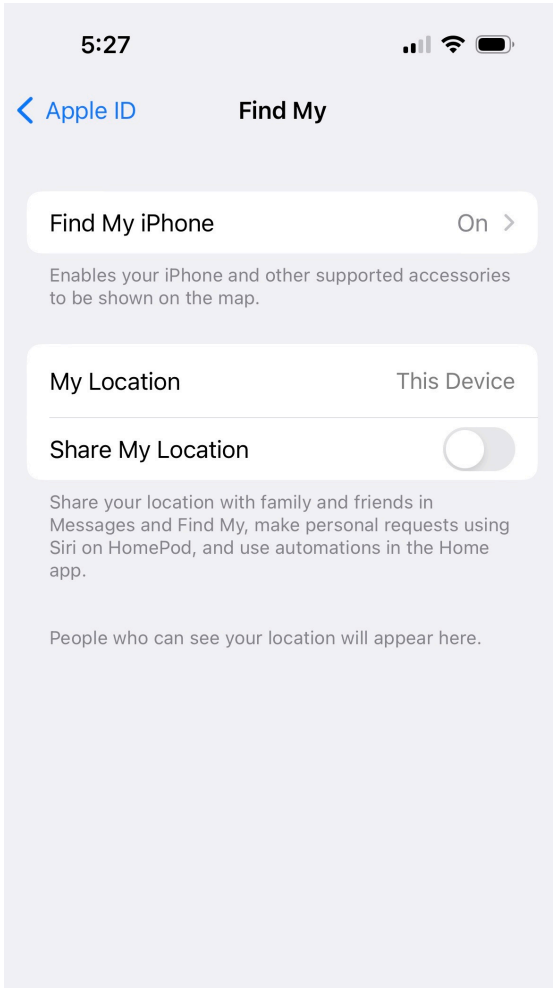
Securing your devices is a priority

- Enable face or touch ID along with a passcode
- Enable “Find My” setting so device can be located if lost/stolen and allow your device to be removed from your account, if needed
- Enable two-factor authentication for your Apple ID
- Disable lock screen notifications for messaging and email. Blocks display of personal and log-in information if your device is stolen.

Settings > Face ID & Passcode

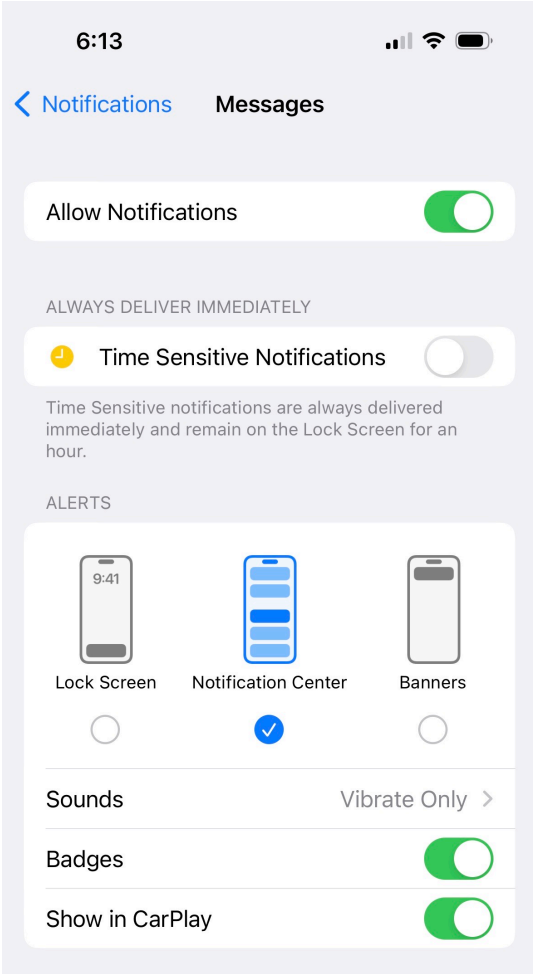


Apple ID > Find My



Apple ID > Password & Security > Two-factor authentication

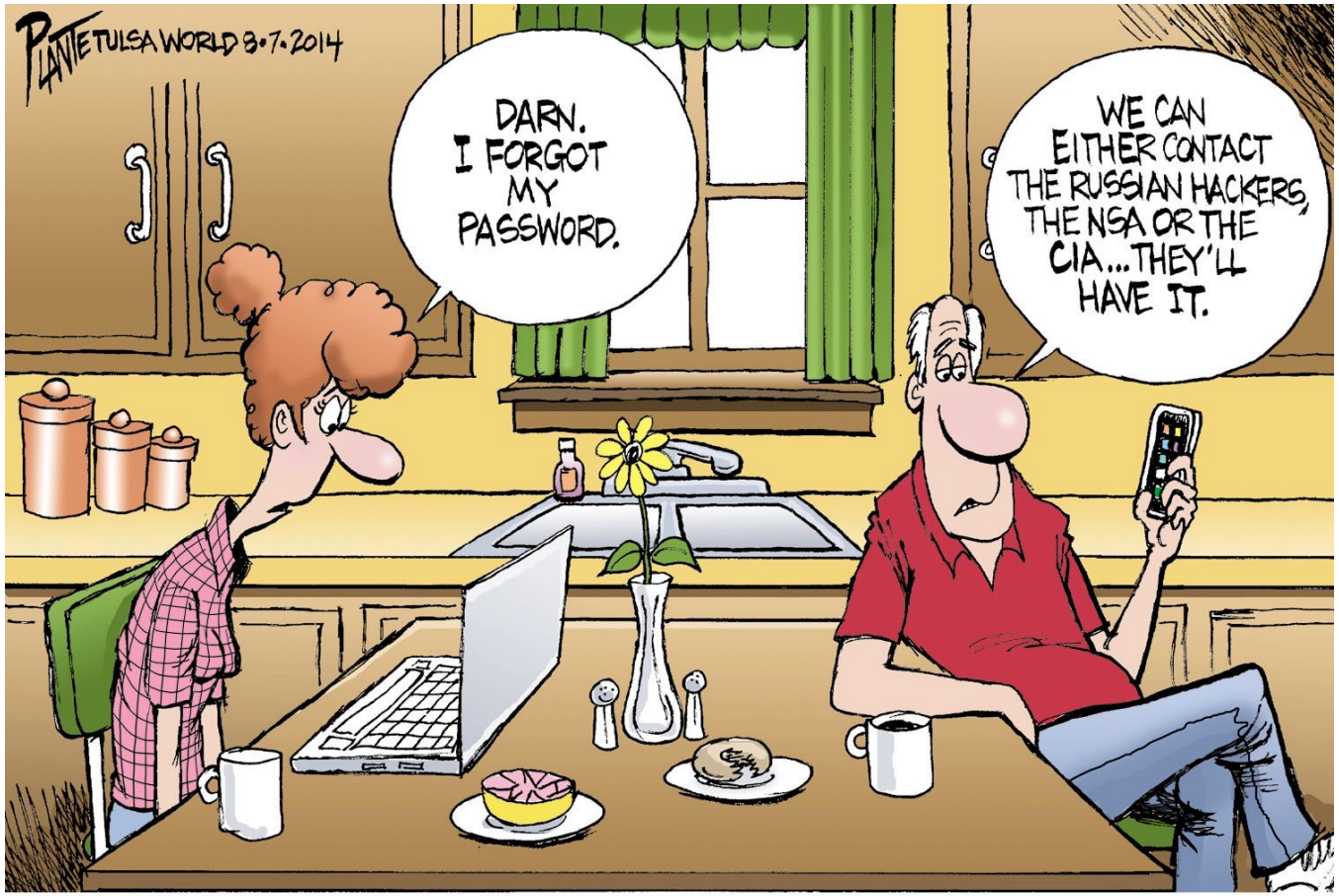
Settings > Notifications > App setting



Improve log-in security to protect your accounts

- Use different usernames for each account, if possible
- Avoid usernames that contain personally identifiable information (e.g., name, address)
- Use a unique, random and long password for each account
- Enable two-factor authentication, if available

If you don’t manage your passwords, someone else will



A password manager is a better approach

- More secure than password savers from Apple and Google
- Creates unique, random passwords for each online account
- Auto populates usernames and passwords when logging in
- Supports different devices and browsers

Roger Buffle Jr. supplies his father with yet another computer password.

Password manager features to look for

- Supports your devices, browsers and operating systems
- Supports at least 20-character random passwords for each account
- Uses a master password to lock and unlock your password vault
- Supports face and touch ID for enhanced log-in security
- Uses 256-bit AES encryption to protect your online password vault
- Works if the password service is offline
- Provides ability to share passwords with spouse (may require family account)
- Offers a free trial so you can try the software before purchasing

Leading password manager products

- 1Password
- Roboform
- Keeper
- Bitwarden
- Proton Pass
- Lastpass (recently had security breaches)

Set up email to protect your privacy

- For better privacy, security experts recommend using different email addresses for different types of online accounts:
  - Critical, trusted accounts - financial, medical, Apple ID
  - E-commerce accounts – Amazon, etc.
  - Social or untrusted accounts – Facebook, forums
  - Personal communications

- Avoid using email addresses containing personally identifiable information (e.g., name, address) with online accounts

- Reserve use of named email addresses for personal communications

Email aliases offer a flexible approach

- Email aliases allow you to create multiple addresses under your main email account
  - Allows you to partition communications
  - An alias can be deleted if too much spam is received or if an address is compromised

- Email services allow you to create multiple aliases:
  - Apple mail: 3 aliases
  - Microsoft mail: 10 aliases
  - Proton mail: 10 aliases
  - Google mail: 30+ aliases (free service requires separate accounts for each alias)

- Email sent to an alias address is received in your main inbox, so it’s a transparent process

Passkeys are the next step in security

- The current log-in process is complicated, and increasingly vulnerable to attack.
- Passkeys are a physical device used for authentication. Can’t be intercepted or hacked.
- Currently best suited for two-factor authentication. Better option than receiving text messages or using software authenticators.
- Worth considering once you’ve improved other security areas and want to experiment with latest technology.

Tips for selecting and using a passkey

- Select a passkey that supports the FIDO2 industry protocol. Allows passkey to be used across multiple sites.

- Needs to support your device's interface ports - USB, Apple lightning or NFC (contactless).

- Yubico's YubiKey 5 series is a leading product: https://www.yubico.com/products/yubikey-5-overview/

- Important! Always register a primary and backup key with an account. Keep the backup key in a safe place.

Use care when making changes

- Enhanced security means taking more responsibility for your devices and accounts. Only make changes that fit your needs and that you're comfortable with.

- Only make a few changes at a time to ensure things work as expected. Document changes in case you want to roll back a setting.

- Backup critical passwords and keys to avoid log-in issues:
  - Save the password manager master password and any secret key so they're safe and accessible
  - Backup your password file to a USB drive stored in a safe place
  - When using passkeys, always register a primary and backup key with your account. Keep the backup key in safe place.

Additional information from the experts

Stay Safe Online security tips:
https://staysafeonline.org/resources/online-safety-basics/

Bank of America security tips:
https://www.bankofamerica.com/security-center/fraud-prevention-checklist/

Charles Schwab security tips:
https://www.schwab.com/learn/story/10-tips-keeping-your-accounts-secure

YouTube channels with helpful security information:

- Shannon Morse
- All Things Secured