AMJ FINANCIAL
WEALTH MANAGEMENT LLC
WEALTH MANAGEMENT MADE SIMPLE

We hope your iPhone never gets stolen. But, just in case....

Here's how to enable security settings, diversify data backups and freeze your credit

By Nicole Nguyen and Joanna Stern, Wall Street Journal

Since reporting on a rash of iPhone thefts that rob victims of their digital lives, we've heard from lots of readers with one big question: How do I protect my precious assets—from photos in the cloud to money in the bank?

Thieves are watching people type in their iPhone passcodes, then snatching the devices, not only making off with the hardware but also gaining access to the precious Apple AAPL -0.55%decrease; red down pointing triangle ID and other important online accounts. Victims have lost thousands of dollars and many have been locked out of their Apple accounts permanently. That means no photos, videos and notes, and even potentially losing access to their AirPods or Apple Watches. Like you, this reporting made us want to do more to safeguard our digital lives and finances in the event of a theft. We believe Apple should reduce the power of the passcode and do more to protect accounts from phone-jackers.

An Apple spokesman said, "We work tirelessly every day to protect our users' accounts and data, and are always investigating additional protections against emerging threats like this one."

Meanwhile, here are four areas where you can protect yourself, with step-by-step instructions on what to do.

Guard your Apple ID

Set a stronger passcode: Your iPhone is the gateway to all your Apple services, and the key to that gateway is likely a simple 4- or 6-digit number. Make it less snoopable: When changing your passcode in Settings, tap Passcode Options, then Custom Alphanumeric Code to enter numbers *and* letters. Consider using a screen protector with a privacy filter.

Add a Screen Time passcode: If you apply Screen Time parental controls to yourself, a thief who gets your iPhone passcode would need a second passcode to change your account. In Settings, go to Screen Time and scroll down to set a passcode (one different from your iPhone's). Then tap Content & Privacy Restrictions, enable that and scroll down to the Allow Changes section. Choose "Don't Allow" for passcode, account and cellular data.

With this in place, a thief would have to tap through a convoluted sequence of steps to reset the Screen Time passcode—buying you time to log into iCloud and wipe your device. (More on that process below.)

Use a security key: These USB/NFC keys are strong protection for online accounts, including your Apple ID. Hackers would need the physical key in hand to remotely reset your Apple password.

Guard your passwords

Use a third-party password manager: Passwords saved in Apple's built-in iCloud Keychain can be accessed with the phone's passcode. Delete info for sensitive logins including bank accounts. Then set up an independent password manager, such as 1Password or Dashlane, which asks for a master password if Face ID or Touch ID fails. Install the manager on multiple devices.

Choose a safe authenticator app: A thief can see verification codes sent to your phone number. Instead, use an authenticator app that protects your two-factor codes. Authy lets you use Face ID or Touch ID to open the app; if they fail, Authy requires you to type a preset PIN. Set up Authy on multiple devices in case you lose one of them.

Review recovery contact info: Ensure you can reset passwords for essential accounts if you lose access. For example, if you have a Google account, set up a recovery email and phone number.

Guard your files

Use a secondary cloud service: Victims locked out of their Apple accounts have been devastated to lose their photos and other files stored in iCloud. So back up your cloud backup. In addition to Apple Photos, we use Google Photos. Amazon Photos, Microsoft OneDrive and Dropbox are other options.

Buy a hard drive: If you don't want to pay for another cloud service, buy a good external USB drive. We suggest a solid-state drive like this SanDisk Extreme

Portable (around $100 for one terabyte). It's faster and more durable than a traditional hard drive.

Set up automatic backups: You can manually back up files to a drive by dragging and dropping them or you can use automatic backups. On a Mac, Apple's built-in Time Machine tool does this with specified files on a regular basis. You can automatically include photos you've downloaded to your Mac. On Windows, you can use iCloud for Windows to download your Apple photos. Then you can use Microsoft's built-in Backup and Restore tool.

Guard your money

Hide sensitive information: Some thieves have opened credit cards using victims' Social Security information, which was found on the phone. Search the Notes and Photos apps and remove any sensitive data, such as photos of your passport. (You can save sensitive documents in locked notes or, better yet, a third-party password manager.)

Freeze your credit: Setting up a security freeze ahead of time can prevent interlopers from extending credit in your name. You can enable this free online for the three major credit firms: Equifax, Experian and TransUnion. (You'll have to unfreeze to open a new line of credit.)

Set debit-card limits: Thieves have linked debit cards stored in Apple Pay to Apple Cash to drain financial accounts. Call your bank to lower a debit card's daily purchase and withdrawal limits.

Add PINs to cash and crypto apps: Financial services that might not have the built-in protections of a bank require extra care. You can add protection to Venmo and Cash App by requiring a PIN to log in. For PayPal, enable biometric login in the app's settings. The app will ask for a password if Face ID or Touch ID fails.

Cryptocurrency exchanges typically don't refund stolen money, so set up a separate passcode to protect the Coinbase or Robinhood app in security settings.

If your phone is stolen…

Log into iCloud.com: From any device's browser, go there and enter your username and password. (Make sure you have those memorized!) Click "Find Devices," then select the stolen device. You may want to screenshot the location for authorities. Click Erase iPhone to wipe all of the phone's data remotely.

Suspend your mobile number: Thieves can use your number to get verification codes, so know how to lock your SIM card's cellular service quickly. T-Mobile has a specific number to call, while Verizon and AT&T customers can suspend their service online.

Call your card issuers: Keep a list of your credit- and debit-card providers' phone numbers in a safe place. If your phone is stolen, call them to suspend the cards.

Revoke your phone's access: If you can't wipe your iPhone, log into online services such as Amazon and Google and remove the stolen device from your account.

Securities offered through Triad Advisors, LLC, Member FINRA/SIPC
Investment Advisory Services offered through AMJ Financial Wealth Management LLC
AMJ Financial Wealth Management LLC is not affiliated with Triad Advisors LLC

The information provided for informational purposes only, and does not constitute an offer, solicitation, or recommendation to sell or an offer to buy securities, investment products or investment advisory services. All information, views, opinions, and estimates are subject to change or correction without notice. Nothing contained herein constitutes financial, legal, tax, or other advice. These opinions may not fit to your financial status, risk, and return preferences.