When you select a password, you might choose to store it in a password manager, write it down, or commit it to memory (see "How to remember passwords" [http://www.macworld.com/article/2014040/how-to-remember-passwords-and-which-ones-you-should.html] for some advice). Sometimes, however, things go wrong: You find yourself without access to your password manager, you lose the paper on which you recorded your passwords, or you forget a password you thought you memorized. Or maybe someone tries to break into one of your accounts, and after a few unsuccessful attempts at entering your password, the site locks out further access until you can confirm your identity.

In all those cases, online services need a secondary way of granting you access to your account or your data when you don’t have (or can’t use) your password. Sometimes—especially in lower-security situations such as access to an online publication or discussion forum—the provider lets you click a link that results in your existing password, a new password, or password-reset instructions being sent to the email address you have on file. When those simple mechanisms are considered too insecure, the site may ask you to respond to verification questions for which you’ve previously provided the answers.

Unfortunately, password-reset messages and verification questions come with their own problems and risks. You can reduce your chances of being hacked—or being unable to respond correctly to one of these questions—by following a few simple tips.

Prevent password-reset mischief
Of all your passwords, the one for your email account may be the most valuable. That’s because whoever has access to your email account will be able to read and...
click links in any password-reset messages you receive (such as when you click an 'I Forgot My Password' link). A hacker who guessed or stole just that one password could unlock many other accounts and do all sorts of damage. You can limit your risk here in a couple of ways.

**Use a dedicated password-reset account:** Consider setting up a new email account for yourself (using a free service such as Gmail (https://mail.google.com)) with an address that you’ll never share or post publicly. Use this account only when prompted to supply an email address for the purpose of verifying or resetting your passwords. That way, even if someone breaks into your main email account, the security of your other accounts won’t be compromised.

**Take extra care with your email account password:** Be sure to choose an especially secure password for your email account. Make sure to set your email client to communicate securely with the mail server—using Secure Sockets Layer, or SSL, protocols for example—so that your password never travels over the air unencrypted. In Apple’s Mail, select Mail > Preferences, click Accounts, choose an email account from the list, and click Advanced. Here you’ll see the option Use SSL.

**Question the questions**

Security questions—such as the timeless classic “What is your mother’s maiden name?”—are supposed to have answers that you’ll never forget but that most other people won’t know or be able to guess. Unfortunately, most of the questions from which you can choose aren’t secure at all.

Your mother’s maiden name is a matter of public record, and nearly anyone can learn it online in a few minutes. If you ever wrote a blog entry or a Facebook post about your first pet, your favorite teacher, or other common security question topics, those facts are in the public domain too. To make matters worse, some questions invite ambiguous answers, which could work against you. Where did you meet your spouse? That might be “in New York” or “at a baseball game” or “at Yankee Stadium,” for example. Years from now, will you remember which answer you gave?

**Devise memorable lies:** To address such problems, there’s only one right way to answer verification questions—lie. And don’t just lie, but come up with one or more answers that follow the same rules as other passwords to prevent guessability; use either a reasonably long (but memorable) phrase or a series of random characters. So, what was the name of my first pet? Why, it was bookends-qualitative. My mother’s maiden name? Her dad was Mr. E27jrdU8. My favorite car? I loved my 1986 Toyota Recalibration Cantaloupe. It doesn’t matter what answers you give, as long as you and you alone know what they are, and can supply the same ones you entered previously if asked.

I know one security expert who says he normally uses the same pseudo-random answer everywhere, although some companies (including Apple) require you to provide different answers to each of several questions—meaning you have even more password-like data to keep track of. Of course, you can write down your answers or store them in a password manager, but then the same problems that prevent you from accessing your password could prevent you from accessing your security answers.

You might make up a little story for yourself about fictional parents, cars, pets, and the like that you can memorize and then draw on when asked for security answers on different sites. Ultimately, since you’re not going to be giving truthful answers, you should go out of your way to remember which lie(s) you told.
Keep them phone friendly: Remember that you could wind up in a situation where you’ll have to supply these answers over the phone. If that should happen, both you and the person on the other end will have an easier time coping with a series of plain-English words than a bunch of random characters.

How to change your security questions and answers

Each service that uses security questions has its own procedure for choosing the questions and answers (and for changing them after the fact). Check the FAQ pages on the websites for your bank and other important accounts to see how to modify your responses.

Update your Apple info: To change the questions or answers for an Apple ID (which you use for iCloud, among many other purposes), go to the Apple ID page (https://appleid.apple.com/), click Manage your Apple ID, enter your username and password, and click Sign in. On the left, choose Password and Security. Answer your existing security questions, and click Continue. Then you can choose new questions and answers (remember, no two answers can be the same) and also edit your Rescue Email Address if you like. Click Save when you're done.

Update your Google info: If you have a Google (https://mail.google.com/) account (for Gmail and other services), log in as you normally would. Click the gear icon in the upper-right corner of the window and choose Settings from the
pop-up menu. Click Accounts and Import followed by Change password recovery options. Under Security question, click Edit. Choose one of the existing security questions or write your own, and fill in your answer. If you also want to change your secondary address, click the Edit link in the ‘Recovery email address’ section and fill in the new address. Then click Save.

**RELATED STORIES**

- [Security in the iCloud age](/article/1168035/security_in_the_icloud_age.html)
- [Review: Refined iOS 6 highlighted by stunning Maps overhaul](/article/2010065/review-refined-ios-6-highlighted-by-stunning-maps-overhaul.html)

**27 comments**

Sort by: OLDEST FIRST NEWEST FIRST MOST RECOMMENDED

**btoole**  
12/03/2012 05:52 AM PST

I am surprised the article does not mention Google's two factor authentication. Google Authenticator running on my iPhone authenticates me to all Google services, Dropbox and a bitcoin site. Awesome actually :-)  
recommend | reply | report abuse

**FlopTech**  
12/02/2012 12:23 PM PST

Re: "Use a dedicated password-reset account"

Yahoo email has "disposable" addresses. You essentially create an alias that sends email to your main Yahoo email. If/when you start to get spam sent to that disposable address, you disable it and create a new one. Works perfectly.

Re: "Devise memorable lies"

Just say your honeymoon was in Kabul, Afghanistan. Especially if you're not married.

recommend | reply | report abuse

**FlopTech**  
12/02/2012 12:18 PM PST

... We can't keep all our passwords on one machine. It just doesn't work.

There are versions of SplashID for iPhone and iPad, and they sync information wirelessly to your desktop / laptop. OS X SplashID Safe must be running. Doesn't use iCloud (yet).

recommend | reply | report abuse

**FlopTech**  
12/02/2012 12:01 PM PST

We love SplashID. Have been using it for many years, works perfectly.