Passwords Are Changing: Longer, Unique —and Sometimes No Password at All

Passwords have been protecting computer accounts for decades, and for much of that time we've been given some thoroughly annoying advice about creating them. Use uppercase and lowercase letters. Add a number. Include a special character. Change the password every few months. Don't write it down. And, of course, don't use the same password twice.

The result was predictable. People created passwords they could remember, reused them everywhere, or wrote them on a piece of paper next to the computer. Fortunately, cybersecurity thinking has changed. Today's advice is both more practical and more secure: **make passwords long, make them unique, let a password manager remember them, use multifactor authentication, and consider passkeys when they're available.**

Why Passwords Get Stolen

We tend to imagine a hacker sitting at a keyboard cleverly figuring out our password one character at a time. That can happen, but criminals have easier ways to obtain passwords. A phishing site can simply ask you for one. Malware can steal credentials. A company's customer database can be breached, exposing thousands or millions of usernames and passwords at once.

Criminals can also use automated programs to try enormous numbers of possible passwords. Common choices such as `password`, `123456`, a pet's name or a simple word followed by a number aren't much of an obstacle.

This creates another problem. If you use the same password for several accounts, a password stolen from one company may unlock accounts at other companies. Criminals routinely try stolen username-and-password combinations against other services. That means the password protecting an unimportant shopping account shouldn't also be protecting your email, bank or other important accounts.

Longer Is Better

For years, users were taught that a password such as `J$7x!2Qp` was wonderfully secure because it contained uppercase and lowercase letters, numbers and symbols. The trouble is that

passwords like that are difficult for humans to remember. Modern guidance puts much more emphasis on **length**. A longer password or passphrase can be both easier to remember and harder to guess than a short collection of keyboard gymnastics.

A passphrase might consist of several unrelated words or a memorable phrase that isn't a familiar quotation, song lyric or expression. The important thing is to avoid information that someone could easily associate with you. Your name, birthday, address, children's names and favorite sports team aren't good raw material if that information is readily available elsewhere.

And don't simply take a good long password and use it everywhere. **Every important account should have its own password.**

Let the Computer Remember for You

At this point you may see the obvious problem. If every account has a different long password, how are you supposed to remember them all? You aren't.

A **password manager** stores your passwords and can create strong, unique ones for your accounts. Instead of remembering dozens of passwords, you protect access to the password manager itself and let the software handle most of the memorization. Modern Apple devices, for example, include Apple's Passwords system, while Google and other companies offer similar password-management services. Independent password managers are also available.

A password manager has another important advantage: it removes the temptation to create easy passwords merely because you have to remember them. If the computer is doing the remembering, a password can be long, random and unique without becoming a daily nuisance.

Add Another Lock with Multifactor Authentication

A password asks, in effect, **What do you know?** Multifactor authentication adds another question. Commonly called **MFA** or **two-factor authentication**, it requires another form of verification in addition to the password. After entering your password, for example, you might approve the login on a trusted device or enter a temporary code generated by an authenticator.

The great advantage is easy to understand. Suppose a criminal obtains your password through a data breach. If the account also requires another form of authentication, the stolen password alone may not be enough to get in. This is particularly important for your primary email account, financial accounts and other services that contain sensitive information.

There is one important warning: **never give an unexpected caller or message sender your authentication code.** A scammer who asks for that code may already have your password and need only the second factor to complete the login.

Meet the Passkey

The most interesting development in password security may eventually make the traditional password much less important. A **passkey** allows you to sign in using security credentials stored on a trusted device rather than typing a conventional password into a website. Depending on the device, you may approve the login using a fingerprint, facial recognition, device PIN or another familiar method.

Passkeys have an important advantage against phishing. A fake website can imitate your bank's login screen and trick you into typing a password. A properly implemented passkey is associated with the genuine website and isn't simply a secret phrase that you can accidentally type into an impostor's page.

With a **passkey**, there is no password for you to type, copy, tell someone, or accidentally hand over. The passkey stored on your Mac, iPhone, or password manager is cryptographically tied to the **real website** for which it was created.

Suppose your real bank is `mybank.com`, but a phishing email sends you to a convincing fake at `my-bank-login.com`. With a password, you might be fooled and type your credentials into the fake page. With a passkey, your device essentially says, **"I don't have a passkey for this website."** The fake site cannot persuade your device to use the passkey belonging to `mybank.com`.

Apple, Google, Microsoft and many major websites now support passkeys, although passwords aren't disappearing overnight. For the foreseeable future, most of us will probably use a mixture of passwords, password managers, multifactor authentication and passkeys.

What About Writing Passwords Down?

Traditional advice insisted that you should never write down a password. That rule deserves some common sense. Leaving your banking password on a sticky note attached to a laptop in a busy office is obviously a bad idea. But for a home user, a securely stored written recovery record may be considerably safer than using `Fluffy123` for twenty different accounts because it's the only password you can remember.

The real objective isn't to obey an absolute rule about paper. It's to prevent unauthorized people from obtaining your credentials. A password manager should handle everyday password storage, while important recovery information can be kept somewhere physically secure.

Protect the Password That Protects Everything Else

Your **email password** deserves special attention. Email accounts frequently receive password-reset links for other services. If a criminal takes control of your email, that person may be able to reset passwords elsewhere and gradually take over more of your digital life.

Protect your primary email with a strong, unique password or passkey and multifactor authentication. Never reuse its password on another website.

Likewise, protect your password manager carefully. It contains the keys to many of your other accounts, so the password or other authentication protecting it deserves special treatment.

Make Security Easier on Yourself

Good password security shouldn't require an extraordinary memory. Technology has finally begun to recognize that human beings aren't particularly good at memorizing dozens of complicated strings of characters.

So don't fight your memory. Let a password manager create and remember unique passwords. Turn on multifactor authentication for important accounts. Use passkeys when reputable services offer them. Protect your email account especially carefully, and never surrender a password or authentication code merely because an unexpected message asks for it.

The old approach was to make passwords complicated enough to frustrate hackers, which frequently frustrated users instead. The better approach is to make your accounts difficult for criminals to enter while making them reasonably easy for **you** to use.

That's cybersecurity progress I can live with.