SECURITY Smart™
NEWSLETTER
SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

What Is Two-Factor Authentication, and When Do I Need It?

TWO-FACTOR authentication, or 2FA if you're into jargon, is a method of establishing access to an online account or computer system that requires users to provide two different types of information. A factor in this context means a way to convince a computer system or online service that you are who say you are, so the system can determine if you have the rights to access the data services that you're trying to access.

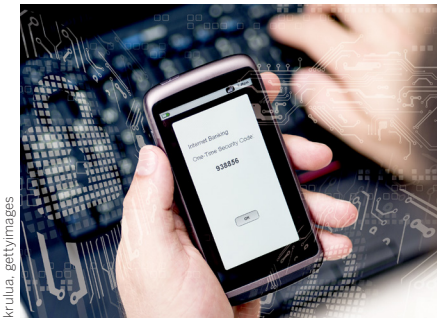
By far the most common authentication factor in use today is the single-factor authentication username/password pair. With 2FA, you need to provide a password and also prove your identity in some other way to gain access.

As passwords have become increasingly less secure, more and more individuals are moving to 2FA to secure their digital lives—and many service providers are encouraging or mandating the shift as well.

Why use 2FA?

Adding a step just makes logging into your account more difficult. So why bother?

For one thing, millions of email address/password pairs are available on the dark web as a result of major data breaches, making passwords less secure. And because most people reuse passwords across multiple sites and accounts, a hacker can gain access by plugging known email address/password pairs into dozens of sites.



krulua, gettyimages

Many sites use so-called security questions, or knowledge-based authentication—"What's your dog's name?" or "Where were you were born?"—as a backup to passwords. But so much personal information is publicly available that a determined hacker can find the answers to these questions for a compromised account. And more importantly, those questions aren't a true second factor and therefore don't provide the layered security of 2FA.

How does 2FA work?

Think of a factor in abstract terms: It's something you know, are or have. That's why using security questions isn't the same as having real 2FA; you're just backing up something you know with something else you know.

True 2FA pairs the first authentication factor, something you know—usually a password—with one of the other two factors, which are entirely different: Something you have might be a code texted to your cell phone, for example; something you are could be a fingerprint or a retina scan.

How do I get 2FA?

As a consumer, figuring out how to enable two-factor authentication for all your accounts can be daunting. Apple, Microsoft, Google, all the major social media sites, Amazon, popular services like Slack and Dropbox, and video games like Fortnite all offer 2FA. A quick web search should lead you to instructions for how to enable 2FA on your accounts. And you can always ask your employer's IT team for advice.

Taking the extra step for security now can save you a lot of headaches in the future.