PROTECTING YOUR ACCOUNTS EVEN IF YOUR PASSWORD IS COMPROMISED.

Two-factor authentication (or "2FA") is a way to let a user identify him or herself to a service provider by requiring a combination of two different authentication methods. These may be something that the user knows (like a password or PIN), something that the user possesses (like a hardware token or mobile phone), or something that is attached to or inseparable from the user (like their fingerprints).

You probably already use 2FA in other parts of your life. When you use an ATM to withdraw cash, you must have both your physical bankcard (something you possess) and your PIN (something that you know). Right now, however, many online services only use one factor to identify their users by default—a password.

How does 2FA work online?

Several online services—including Facebook, Google, and Twitter—offer 2FA as an alternative to password-only authentication. If you enable this feature you'll be prompted for both a password and a secondary method of authentication. This second method is typically either a one-time code sent by SMS or a one-time code generated by a dedicated mobile app that stores a secret (such as Google Authenticator, Duo Mobile, the Facebook app, or Clef). In either case, the second factor is your mobile phone, something you (normally) possess. Some websites (including Google) also support single-use backup codes, which can be downloaded, printed on paper, and stored in a safe location as an additional backup. Once you've opted-in to using 2FA, you'll need to enter your password and a one-time code from your phone to access your account.

Why should I enable 2FA?

2FA offers you greater account security by requiring you to authenticate your identity with more than one method. This means that, even if someone were to get hold of your primary password, they could not access your account unless they also had your mobile phone or another secondary means of authentication.

Are there downsides to using 2FA?

Although 2FA offers a more secure means of authentication, there is an increased risk of getting locked out of your account if, for example, you misplace or lose your phone, change your SIM card, or travel to a country without turning on roaming.

Many 2FA services provide a short list of single-use "backup" or "recovery" codes. Each code works exactly once to log in to your account, and is no longer usable thereafter. If you are worried about losing access to your phone or other authentication device, print out and carry these codes with you. They'll still work as "something you have," as long as you only make one copy, and keep it close. Remember to keep the codes secure and ensure that no one else sees them or has access to them at any time. If you use or lose your backup codes, you can generate a new list next time you're able to log in to your account.

Another problem with 2FA systems that use SMS messages is that SMS messaging isn't that secure. It's possible for a sophisticated attacker who has access to the phone network (such as an intelligence agency or an organized crime operation) to intercept and use the codes that are sent by SMS. There have also been cases where a less sophisticated attacker (such as an individual) has managed to forward calls or text messages intended for one number to his or her own, or accessed telephone company services that show text messages sent to a phone number without needing to have the phone.

If you're worried about this level of attack, turn off SMS authentication, and only use authenticator apps like Google Authenticator or Authy. Unfortunately this option is not available with every 2FA-enabled service.

In addition, using 2FA means you may be handing over more information to a service than you are comfortable with. Suppose you use Twitter, and you signed up using a pseudonym. Even if you carefully avoid giving Twitter your identifying information, and even if you access the service only over Tor or a VPN, if you enable SMS 2FA, Twitter will necessarily have a record of your mobile number. That means that, if compelled by a court, Twitter can link your account to you via your phone number. This may not be a problem for you, especially if you already use your legal name on a given service, but if maintaining your anonymity is important, think twice about using SMS 2FA.

Finally, research has shown that some users will choose weaker passwords after enabling 2FA, feeling that the second factor is keeping them secure. Make sure to still choose a strong password even after enabling 2FA. See our creating strong passwords guide for tips.

How do I enable 2FA?

This differs from platform to platform, as does the terminology used. An extensive list of sites supporting 2FA is available at https://twofactorauth.org/. For the most common services, you can refer to our 12 Days of 2FA

post, which shows how to enable 2FA on Amazon, Bank of America, Dropbox, Facebook, Gmail and Google, LinkedIn, Outlook.com and Microsoft, PayPal, Slack, Twitter, and Yahoo Mail.

If you want better protection against stolen passwords, read through this list and turn on 2FA for all of the important web accounts you rely on.

Source: https://ssd.eff.org/en/module/how-enable-two-factor-authentication