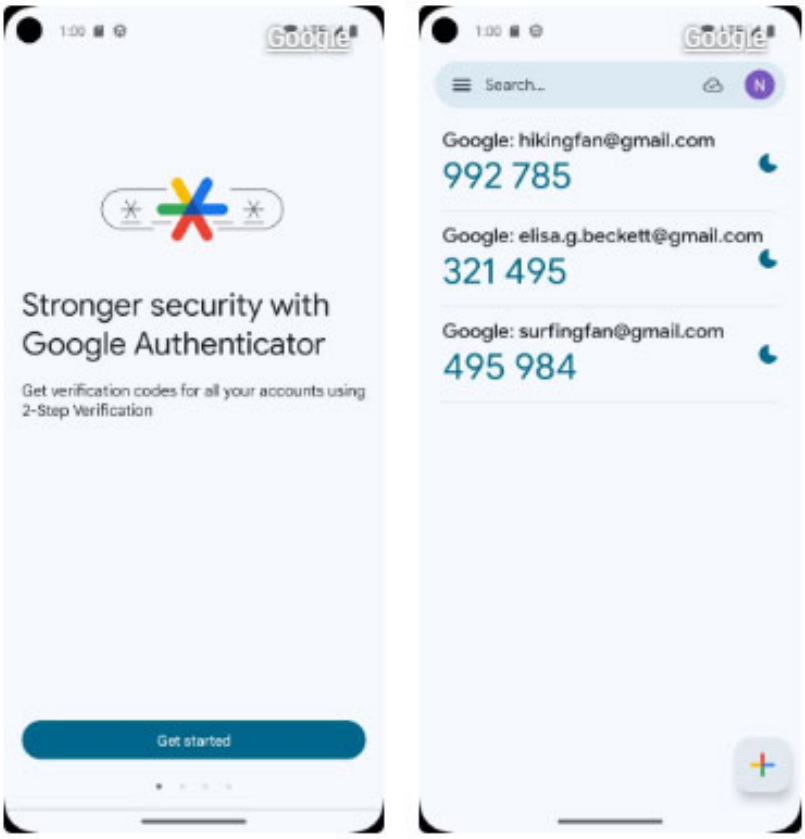
Hackers Hate These 6 Email Settings! Turn Them On Now!

Failing to proactively protect your email can leave an open door that hackers will have a hard time resisting. Fortunately, enabling these settings will help keep hackers at bay and won't take long for them to get their way.

Failing to proactively protect your email can leave an open door that hackers will have a hard time resisting. Fortunately, enabling these settings will help keep hackers at bay and won't take long for them to get their way.

6. 2FA via authenticator app

One of the easiest ways to reduce the risk of your email being hacked is to enable two-factor authentication (2FA) . Even if a hacker guesses your password correctly, they'll have to verify their identity in another way they may not have access to. This is one of the best forms of multi-factor authentication (MFA).



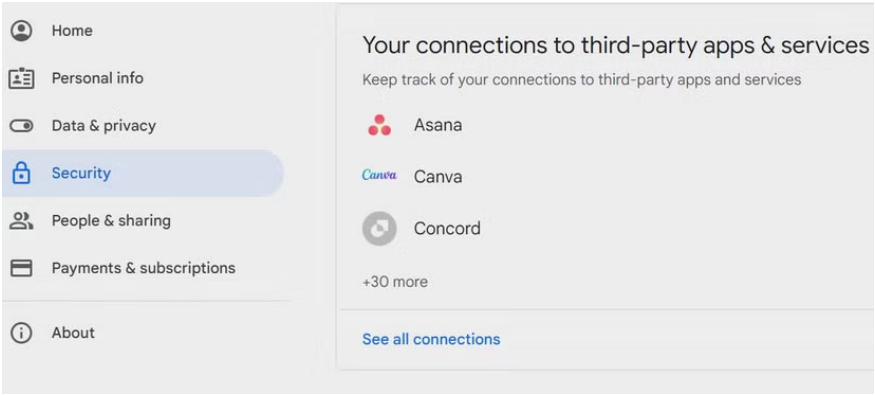
There are a number of ways you can enable 2FA, but we recommend using an authenticator app. For example, Google Authenticator. Many password managers have their own versions, and the differences between them are minimal.

After enabling 2FA through an authenticator app, you'll typically see a changing code that you'll need to enter when prompted. In some cases, you can scan a QR code instead.

5. Remove third-party tool access

Logging into an account with your email address is often easier than setting up a separate profile and creating a new password. But while it's helpful to have easy access to services you use regularly, giving third-party tools access to your email can put you at risk.

While many of the tools you use with your email will have robust security infrastructures, not all do. You should be especially careful when signing up for new tools that haven't been tested for a long period of time. If the app or service eventually becomes outdated and no longer receives updates, hackers may discover the vulnerability.



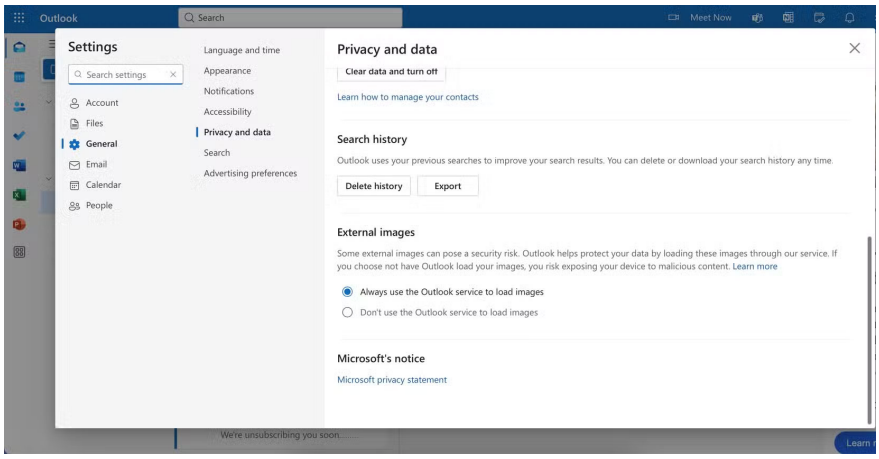
Only keep access to third-party tools that you use regularly. You can go into your email account settings and remove access to apps you no longer want; make it a habit to do this at least once every few weeks. Take the same precautions when logging in with social media credentials!

4. Use the email's external image loading feature

While usually fine, external images can sometimes pose security threats and attack vectors. For example, cybercriminals can insert code or add tracking pixels into the spam they send. Unless you 100% trust the sender (or are clearly from a verified corporate account), you should be cautious about accessing external images in your emails.

Using your email client's image loader can reduce your risk of attack by ensuring your data is secure. Outlook , for example, has a feature that allows you to do exactly this.

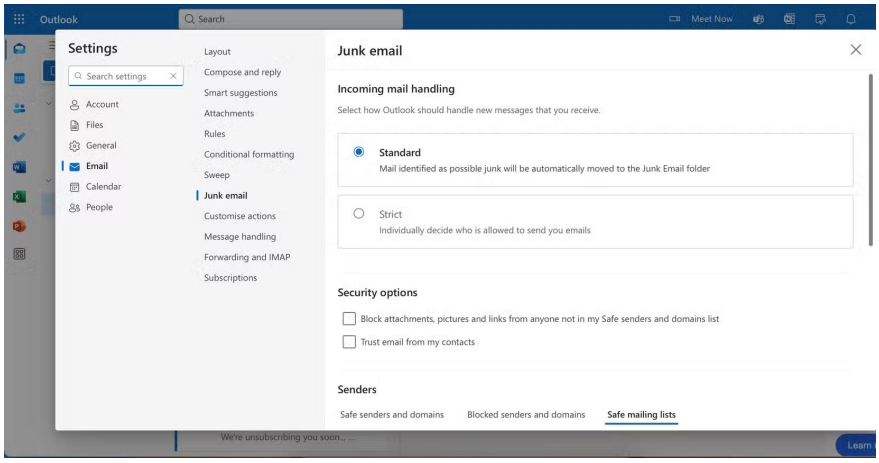
1. Go to **Settings > Privacy and data > External images** .
2. Check the **Always use the Outlook service to load images** option .



Not using this tool is one of many email security mistakes you can make. If your email client doesn't have such a feature, you might want to consider switching to another service.

3. Handle incoming emails strictly

Unfortunately, your email account is the starting point for many scams. You're likely to receive more phishing emails than actual mail, which means you need your email account and service to have excellent spam filters. While many email clients do a good job of filtering spam and phishing emails, they won't catch everything, and you shouldn't trust them to do so.



Instead, you should use them as an initial filter, but then take matters into your own hands. Most email clients allow you to individually select who is allowed to send you emails, using a whitelist method.

Because you have complete control over who can send you emails, you're less likely to fall victim to hackers. Plus, you'll protect yourself from other email security threats, like phishing.

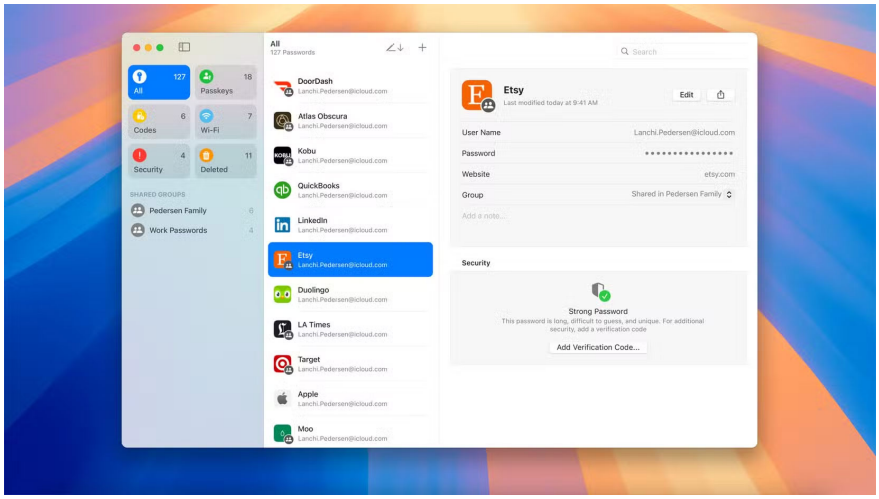
2. Block attachments

While blocking external images will help reduce your risk of being hacked, you may want to go a step further and block attachments from senders you don't trust. With some tools, you can block anyone not on your safe list from sending you images, documents, and other content that could pose a security threat.

In addition to adding safe senders, you can allow attachments from people in your contacts or trusted domains. There is also the option to add safe mailing lists. You don't need to enable all of these features, but it's a good idea to enable at least one of them.

1. Strong password

Even with all the forms of online authentication, having a strong password is still one of the best ways to prevent your email account from being hacked. It's easier than ever these days; password generator apps like Apple Passwords will create a hard-to-guess password for you in less than a minute.



All of your email account passwords should be unique. Even if your password is difficult to guess on one account, you should not reuse it. If your data is compromised, you increase your risk of being hacked into multiple accounts.

You can also switch to a password lock, which in addition to protecting against hackers, can also act as an anti-phishing alternative to passwords.

Protecting your email account from hackers doesn't have to be a chore. With a few simple steps, you can keep your information safe and continue to enjoy the benefits of email with fewer downsides. Adding more layers of security will reduce the chances of something worse happening.

You finished reading the article "**Hackers Hate These 6 Email Settings! Turn Them On Now!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.