Best practices for security

- Best practices for making a business portfolio more secure
- Turn on the two-factor authentication requirement in your business portfolio
- Share your domain with a partner
- About brand suitability on Meta platforms and Audience Network

Best practices for making a business portfolio more secure

Best practices for making a business portfolio more secure

To help keep your business portfolio secure and protect your business and accounts from bad actors or unauthorized activity, follow these best practices and recommendations.

Security Center recommendations

If you have full control of the business portfolio, you can go to the Security Center to see if you've been urged to take action on any of the following security improvements. You can also track the progress of completing these recommended tasks.

Remove inactive users

Bad actors often target inactive accounts in an effort to gain access to a business portfolio. Remove people who haven't logged into the portfolio within the past 90 days, especially those with full control of the portfolio. Learn more about how to remove people from your business portfolio.

Close or remove inactive ad accounts

Bad actors are more likely to target ad accounts that haven't run ads within the last year. Close or remove ad accounts you no longer need. **Note**: Ad accounts can't be deleted from the portfolio.

Learn more about how to close an ad account that's in a business portfolio.

Remove users without two-factor authentication

People who don’t have two-factor authentication set up pose a security risk. Remove them from the portfolio until they have set it up using their Facebook account.

Remove users with public email domains

Bad actors often use public email domains to create email addresses anyone can get in order to gain access to a business portfolio. Remove users whose email addresses aren’t related to your business.

Limit number of users with full control of the business portfolio

Having too many users with full control of the business portfolio may pose a security risk. Limit full control to only those who need it, ideally 10 or fewer people.

Learn more about how to change people’s access to a business portfolio.

Add another review of your ads with peer approval

Bad actors often run unauthorized ads, and these ads may be published without requiring a peer review. To require a review by a trusted user before ads are published, set up ad account and domain security in peer approval.

Learn more about how to add a second review with peer approval

Remove users detected with possible malware

Malware is malicious software that could lead to harmful activity in a business portfolio. Remove people from the portfolio who may have malware on one of their devices.

Learn more about protecting your accounts from malware.

Review shared credit lines with suspicious activity

Bad actors may gain access to shared credit lines to run their own ads. Review your credit lines and the businesses they’re shared with. Remove any that have suspicious or unauthorized activity.

Learn more about billing and payments.

Other recommendations

Here are some additional actions you can take to help make your business portfolio more secure.

Set up passkeys

Set up passkeys for every Facebook user in your business portfolio, particularly admins. Passkeys are a stronger, more secure two-factor authentication method than SMS codes, helping protect access to your portfolio settings.

Learn more about how to create a passkey to access your portfolio settings.

Avoid two-factor authentication issues

To avoid login issues with two-factor authentication:

- Use an authenticator app. Remember to back up your authenticator app in case you lose access to, or switch, your device.
- Set up multiple methods, including saving your recovery codes. This way you can still access your business portfolio, even if you lose one of the recovery methods.
- Update your phone number in your Facebook account settings after changing your mobile phone number to make sure you can receive security codes by text message or SMS.

Learn more about how two-factor authentication works on Facebook.

Make sure 2 people have full control of the business portfolio

It's recommended (but not required) that 2 active people have full control of a business portfolio. Also known as "second admin approval," this provides additional security by adding a second layer of approval to sensitive actions, such as requests to share credit lines or change the access of someone with full control of the portfolio.

Having more than one person with full control also ensures someone else has top-level access to the portfolio in the event that one of your accounts or business assets shows suspicious activity.

Learn more about how to change people's access to a business portfolio.

Report suspicious or unauthorized activity

If you notice suspicious or unauthorized activity, contact our support team.

Audit people's level of access

Perform an audit of people in your portfolio to make sure they don't have more permissions than they need. People with full control of the portfolio can export a file with users' permissions from the **People** tab in Meta Business Suite's **Settings**. You'll also find information on when they were last active and whether they have two-factor authentication turned on. **Note:** People who have been invited to join your portfolio but have not yet accepted are not included in this report.

Learn more about how to download people permissions.

Monitor business portfolio activity

Review your business history, a file of important events that occurred in your portfolio, to look for any unauthorized activity, such as changes to portfolio details, business assets and people. You can download your business history from the **People** tab or **Business info** tab in Meta Business Suite's **Settings**.

Learn more about how to download your business history.

Common support topics

About advertising restrictions

Business Help Center

Troubleshoot a disabled or restricted account

Business Help Center

About Meta Business Support Home

Business Help Center

Fix a failed payment issue on Meta

Business Help Center

Turn on the two-factor authentication requirement in your business portfolio

Turn on the two-factor authentication requirement in your business portfolio

Two-factor authentication can help protect your account from unauthorized access.

If you created your business portfolio less than 90 days ago, you can choose to require two-factor authentication for people in your account.

If two-factor authentication is required for your business portfolio, people must also turn on two-factor authentication to access the business portfolio. **Note:** For security reasons, turning on two-factor authentication is required for certain business portfolios that are more than 90 days old.

You can share this article with people in your business portfolio for directions on how to turn on two-factor authentication for Facebook accounts.

Before you begin

Only people with full control of the business portfolio can turn on the two-factor authentication requirement.

Turn on the two-factor authentication requirement

1. Go to **Settings** in Meta Business Suite.
2. Click **Business portfolio info**.
3. Scroll down to **Business options.**
4. Click the dropdown menu next to **Two-factor authentication**.
5. Select **Admins only** or **Everyone** to choose who this requirement applies to. To turn off two-factor authentication requirement, choose **No one**.

After you turn on the two-factor authentication requirement, Meta needs to remember your computer and browser info so we recognize it next time you log in. Some browser features block this. If you've turned on private browsing or set up your browser to clear your history every time it closes, you might have to enter a code every time you log in. If you use a third-party app to manage the Pages or ad accounts in your business portfolio, you'll be asked to enter a login code the next time you sign in from the app.

If you've turned on two-factor authentication requirement and get a prompt to enter a code for security purposes, you can generate one from your phone. Learn how to receive a code for two-factor authentication.

Basics

About Security CenterAbout brand safety in Meta Business Suite About domain verification in Meta Business Suite Permissions for block lists

Set Up

Manage publisher block listsTurn on the two-factor authentication requirement in your business portfolioReceive a code for two-factor authentication on Facebook

Share your domain with a partner

Share your domain with a partner

You can give a partner access to your business's domain in Meta Business Suite. Sharing your domain lets trusted partners run and manage ads for your business.

Sharing your domain doesn't give your partner ownership of managing the domain. You can remove your partner's access at any time.

Before you begin

- You must have a business portfolio
- The intended partner must have a business portfolio.
- You can only share a verified domain. Learn more about how to verify your domain.

Share your domain with a partner

To share your domain with a partner's business portfolio in Meta Business Suite:

1. Go to **Settings** in Meta Business Suite.
2. Select the **Brand Safety** tab from the left navigation menu. Then select **Domains**.
3. Select the verified domain you want to share.
4. Click **Assign partner**.
5. Enter your partner's business portfolio ID. The business portfolio ID can be found in the **Business Info** tab.
6. Select whether you'd like to give your partner **Partial access** or **Full control** of your domain.
7. Click **Next.**
8. Click **Done** to finish.

You should see your partner’s information under the **Partners** tab. You can stop sharing your domain with a partner at any time by clicking the trash icon and removing the partner.

Learn more

- Manage ad link editing permissions

About brand suitability on Meta platforms and Audience Network

About brand suitability on Meta platforms and Audience Network

Brand suitability controls help advertisers control where ads are delivered on Meta platforms and Audience Network. You can use brand suitability controls to help you place ads adjacent to organic content and publishers that are suitable to your brand.

There are controls that can be applied to your entire ad account and to specific ad campaigns.

Meta Community Standards

Our goal is to create a safe and welcoming community for the more than 3 billion people who use Meta technologies around the world, across cultures and perspectives. To help achieve this goal, our Community Standards define what content is and isn't allowed on our technologies. Our policies are based on feedback from our community and the advice of experts in fields such as technology, public safety and human rights.

We have around 40,000 people working on safety and security, which includes removing billions of fake accounts a year. We also invest in technology to reduce the spread of false news and help identify content that violates our policies—often before anyone sees it. And we routinely release the Community Standards enforcement report to track our progress to make Facebook and Instagram safe and inclusive.

Monetization Policies

Community Standards apply to everyone and all content on Facebook and Instagram, we also have additional policies to hold creators and publishers accountable. Our Partner Monetization Policies apply at the account level. Learn more about Facebook's Partner Monetization Policies and Instagram's Partner Monetization Policies. They include rules for the content you create, how that content is shared, and how your account receives and makes online payments. Additionally, all content on Facebook and Instagram must comply with our Terms and Community Standards and Guidelines. However, content appropriate for Facebook and other Meta technologies isn't necessarily appropriate for monetization. This content has to follow our Content Monetization Policies—they include prohibited formats, behaviors and restricted categories. This means that not all content on Facebook and Instagram is monetizable.

There are rigorous brand suitability controls, including publisher and content block lists, inventory filters, live stream exclusions and some recent tools that are both at the publisher and content level to allow advertisers greater control over where their ads may appear.

Brand suitability controls

Controls that allow you to manage brand suitability settings directly within the Meta Brand Safety and Suitability Center. Learn more about our brand suitability controls.

Learn more

- Making platforms safer for brands and people
- Best practices for brand suitability

Brand suitability controls, such as inventory filter, help you place ads adjacent to organic content that are suitable for your brand in certain ad placements. We define organic content as content posted without being promoted as an advertisement.

Basics

About brand suitability on Meta platforms and Audience NetworkBest practices for brand suitability About brand suitability controls and transparency toolsManage brand suitability controls within the Meta Brand Safety and Suitability Center from Meta Business SuiteAbout the publisher review processAbout community content reviewsRequest brand safety supportUse brand suitability controls on individual ads or on your whole ad accountMeta's brand safety description of methodologyAbout Feed and In-content brand safety and suitability controls

Publisher List

About partner-publisher listsView or download partner-publisher listsReview partner-publisher lists

Block Lists

About publisher and content block listsCreate a publisher block list in the Meta Brand Safety and Suitability CenterUpload a publisher block list in the Meta Brand Safety and Suitability CenterApply a publisher block list in Meta Ads ManagerApply a publisher block list in the Meta Brand Safety and Suitability CenterBest practices for publisher block list limit warningsBest Practices For Block List LevelsShare publisher block lists

Exclusions

About live video exclusionsAbout content type exclusionsAbout topic exclusions Apply topic exclusions About content from nonpartner-publishersApply content type exclusions

Inventory Filter

About inventory filterUse inventory filter from the Meta Brand Safety and Suitability CenterUse inventory filter in Meta Ads ManagerContent inventory table: in-content placementsContent inventory table: Meta Audience Network

Delivery Reports

About delivery reportsView delivery reports in the Meta Brand Safety and Suitability Center Download delivery reports in Ads ManagerReview delivery reportsAbout approximate impressions