

Trusted Device

A trusted device is a phone, tablet, or computer that you have previously used and marked as trusted after successfully signing in.

When using a trusted device, you may not need to complete two-factor authentication every time you log in.

For example, after entering your password and verification code once on your personal laptop, you can choose:

“Trust this device” or “Don’t ask again on this device”

The system then remembers that device for future sign-ins.

How Trusted Devices Work

When you trust a device:

1. You complete the normal sign-in and verification process
2. A secure record is stored in your browser or device
3. On future logins from the same device and browser, you may not be asked for another verification code

You may still be asked to verify again if:

- you clear your browser cookies,
- use a different browser,
- sign in from a new location,

- your device changes significantly,
 - or your trusted session expires.
-

Is a Trusted Device Safe?

Trusted devices are generally safe for personal devices that only you use, such as:

- your personal laptop,
- home computer,
- or private mobile phone.

It is not recommended to trust:

- public computers,
- shared family devices,
- internet café computers,
- or devices you do not control.

If you ever lose access to a trusted device, you should remove it from your account security settings if possible.