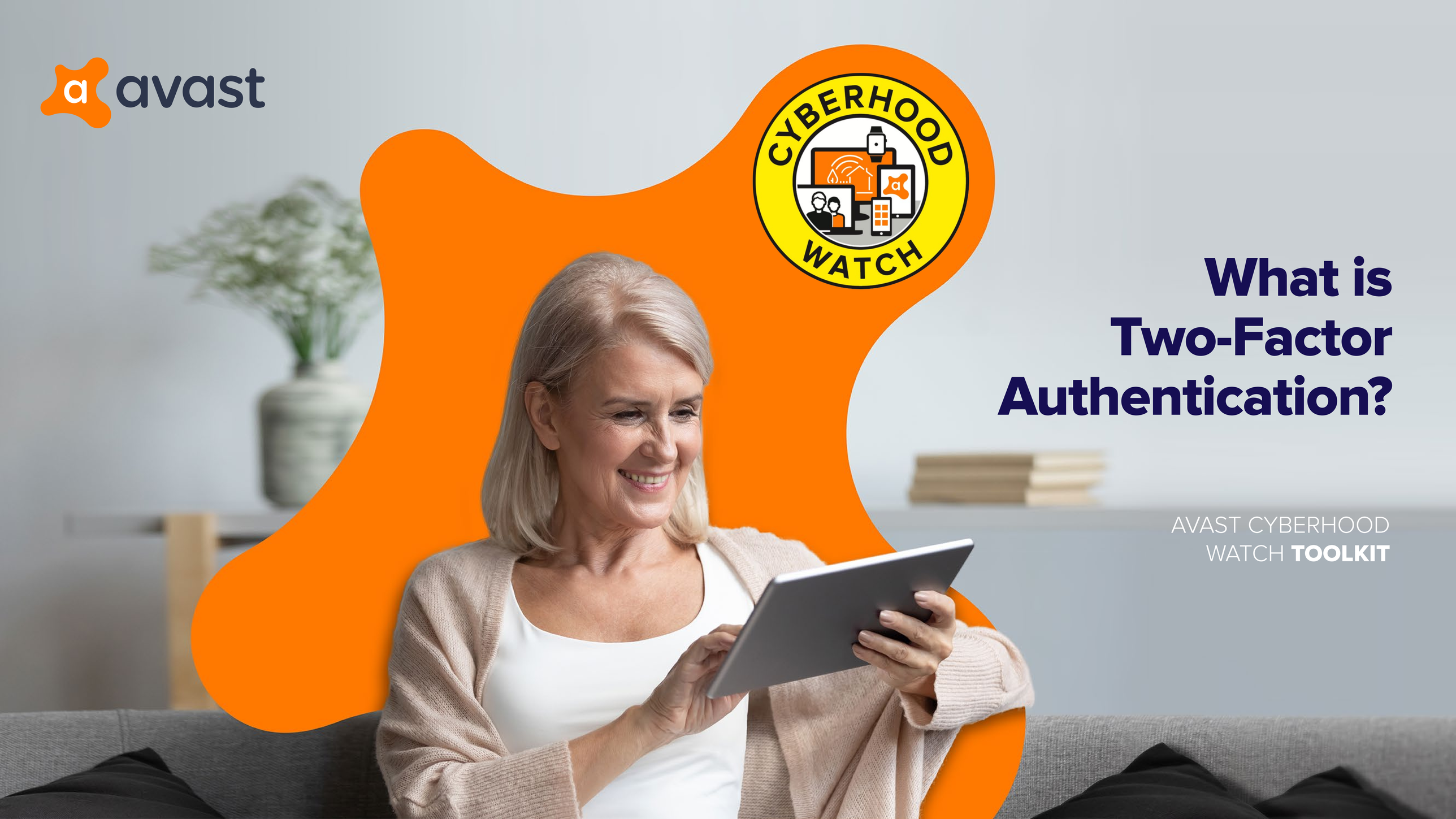

What is Two-Factor Authentication?

AVAST CYBERHOOD
WATCH **TOOLKIT**

What is Two-Factor Authentication (2FA)?

Most online accounts today (banks accounts, email accounts, social media accounts), include technologies that are designed to verify your identity so only you can access them. Among these technologies is something called factors of authentication. There are three classic “factors” that online services use for customers to prove they are who they say they are:

1. Something you know e.g. a password
2. Something you have e.g. a key fob, a card or token
3. Something you are e.g. a fingerprint, face or retina scan

The idea behind factors of authentication is that it should be harder to steal multiple factors than steal one. Generally speaking, the more factors presented, the more likely it is that the person’s identity is true, and the harder it is for an adversary to fraudulently access an online account.

Two-factor authentication (2FA) uses two of the factors above, usually something you know (a password) and something you have (a key fob, although many services today provide this second factor via email or text message as a numerical code). This means that somebody needs to steal your password and your numerical code to access an account with 2FA enabled. To do this simultaneously is hard.

A common analogy used to describe 2FA concerns a house. If you need to use a physical key and a digital code to enter it, a burglar who steals your key without also stealing the code will be unable to break in. The same principle applies in the online world as well.

TOP TIP

Where possible, always enable 2FA from the security settings of your accounts that hold personal and sensitive information. 2FA is particularly important when authorising transactions through online banking, and logging into email and social media accounts.