MULTI-FACTOR AUTHENTICATION

Devices and accounts are important tools that help us stay connected. But they also contain a lot of personal information that you don't want to fall into the wrong hands. So how do you ensure your private information stays private? Go beyond just a password by enabling multi-factor authentication, which requires additional verification (like a PIN or fingerprint) to access your devices or accounts.

MULTI-FACTOR AUTHENTICATION IS ALL ABOUT YOU

WHO YOU ARE

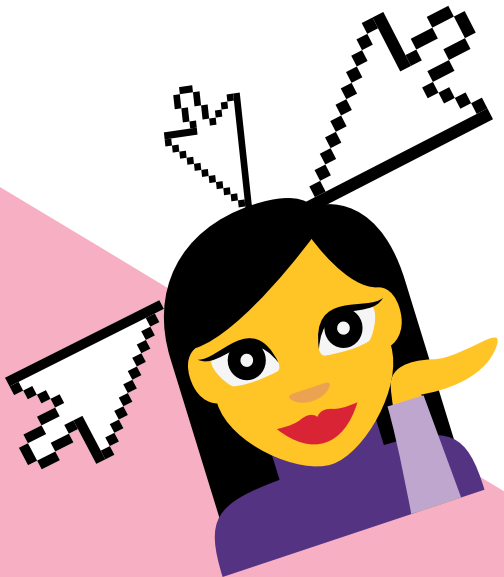
- Fingerprint scanners
- Voice verification
- Facial recognition

WHAT YOU KNOW

- Security questions
- Passwords and passphrases
- PINs

WHAT YOU OWN

- SMS authentication
- Application-based authentications
- Hardware tokens



DID YOU KNOW?

1 in 3 Canadians use multi-factor authentication[1]

A simple 2-step verification can protect you from:

- 100% of automated bots
- 96% of phishing attacks
- 76% of targeted attacks[2]

81% of hacking-related data breaches are due to weak or stolen passwords[3]

HOW YOU CAN PROTECT YOURSELF ONLINE

Enabling multi-factor authentication can help you keep your data safe from cyber criminals.

Some authenticators, like SMS or application-based authentications, can make you aware of someone attempting to access your account.

[1] Public Safety Canada, Survey of Internet Users Regarding Cyber Security, EKOS Research Associates, 2018

[2] New research: How effective is basic account hygiene at preventing hijacking, Google Security Blog, 2019

[3] 2017 Data Breach Investigations Report, Verizon, 2017

Communications Security Establishment

Canada