ESTIMATES SAY A BREACH OF 50 MILLION RECORDS OR MORE COULD COST AS MUCH AS $350 MILLION IN DAMAGES, AND BREACHES ARE EXPECTED TO COST COMPANIES $9.2 TRILLION IN 2019.

MULTI-FACTOR AUTHENTICATION MAY PROTECT YOUR INFORMATION IF YOUR CREDENTIALS ARE COMPROMISED.

MULTI-FACTOR AUTHENTICATION REQUIRES AT LEAST TWO VERIFICATION TECHNOLOGIES USING THREE IDENTIFIERS UNIQUE TO YOU.

WHAT YOU KNOW
Create passwords or phrases that are 12 characters or more; easy to remember, but difficult to guess. PINs should be at least 6 digits long. Never use the same password/passphrase for multiple sites. Use an encrypted password management tool to help you organize and track your passwords.

WHAT YOU HAVE
Authenticate your identity using a physical item or something only you have access to at the time you request access, such as a debit card, time-sensitive PIN or password, token, or mobile phone. Time-based password generators are available for most devices.

WHO YOU ARE
Biometric recognition software is quickly becoming standard on most mobile devices, including phones, laptops, and tablets. From fingerprint scans to retina and face-recognition, this level of authentication can thwart a breach even if your passwords or devices have been compromised.