Are you protecting your firm and clients with multi-factor authentication (MFA)?

Hacking. Phishing. Tax fraud. Firms of all sizes and specialties are regularly targeted by cybercriminals using increasingly sophisticated methods — often causing devastating results for the victimized businesses.

The good news is MFA is a seriously powerful way to protect yourself, your firm, and your clients. At Thomson Reuters, we help you stay one step ahead of the hackers — not only preventing cybercriminals from gaining access to your system, but also alerting you if a suspicious party is using your credentials.

The humbling reality

58% of malware attack victims are categorized as small businesses.

Source: Cybersecurity statistics every small business should know in 2018, May 2018

597,000 / $6 billion

The IRS stopped **597,000** confirmed identity theft returns, totaling more than **$6 billion**.

Source: Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress Against Identity Theft, Feb. 2018

80% of data breaches could have been prevented by multi-factor authentication.

Source: Is Your Data Safe? The alarming rate of security non-compliance by employees today: Symantec, 2015

Authenticator to the rescue

Email or text verification is not safe enough, and still leaves you vulnerable to cybercriminal attacks. Give your clients true protection with multi-factor authentication (MFA).

The **Thomson Reuters Authenticator™** app uses MFA to grant a user access only after successfully presenting two of the three following methods of confirmation:

- Something **you know** Ex: Password
- Something **you have** Ex: Smartphone
- Something **you are** Ex: Fingerprint

Take action now

Stand strong as your clients' first line of defense against tax fraud. See how you can team up with Authenticator to protect your clients' data at **tax.tr.com/authenticate-now**

THOMSON REUTERS®

TA601452_112022_pd