MFA: BECAUSE TWO ARE STRONGER THAN ONE.

Q. What is multifactor authentication (MFA)?
A. A security enhancement that requires two forms of credentials to gain access to an account.

Q. Why use MFA?
A. There is a hacking attempt every 39 seconds. Annually, 1 in 3 Americans are affected. The average cost of a data breach in the US is $225 per record.

Q. How can hackers steal login information?
A. The easiest and fastest way for hackers to obtain sensitive data is through access to privileged accounts.

Q. Why is MFA critical today?
A. Cybercrime has increased 600% due to the COVID-19 pandemic. Remote work is extremely common and has become a focus for hackers. 43% of all cyberattacks are directed at small businesses. One-quarter of all employees have noticed an increase in fraudulent emails, spam and phishing attempts in their corporate emails since the beginning of COVID-19.

Q. What’s the solution?
A. MFA can prevent over 99.9% of account compromise attacks. With MFA, even if your username or password gets compromised, a hacker won’t gain access without receiving your MFA Security Code.

Sources:
1 - Clark School, University of Maryland; 2 - Ponemon Institute; 3 - Thycotic; 4 - PurpleSec; 5 - Smallbiztrends.com; 6 - Deloitte; 7 - Microsoft;