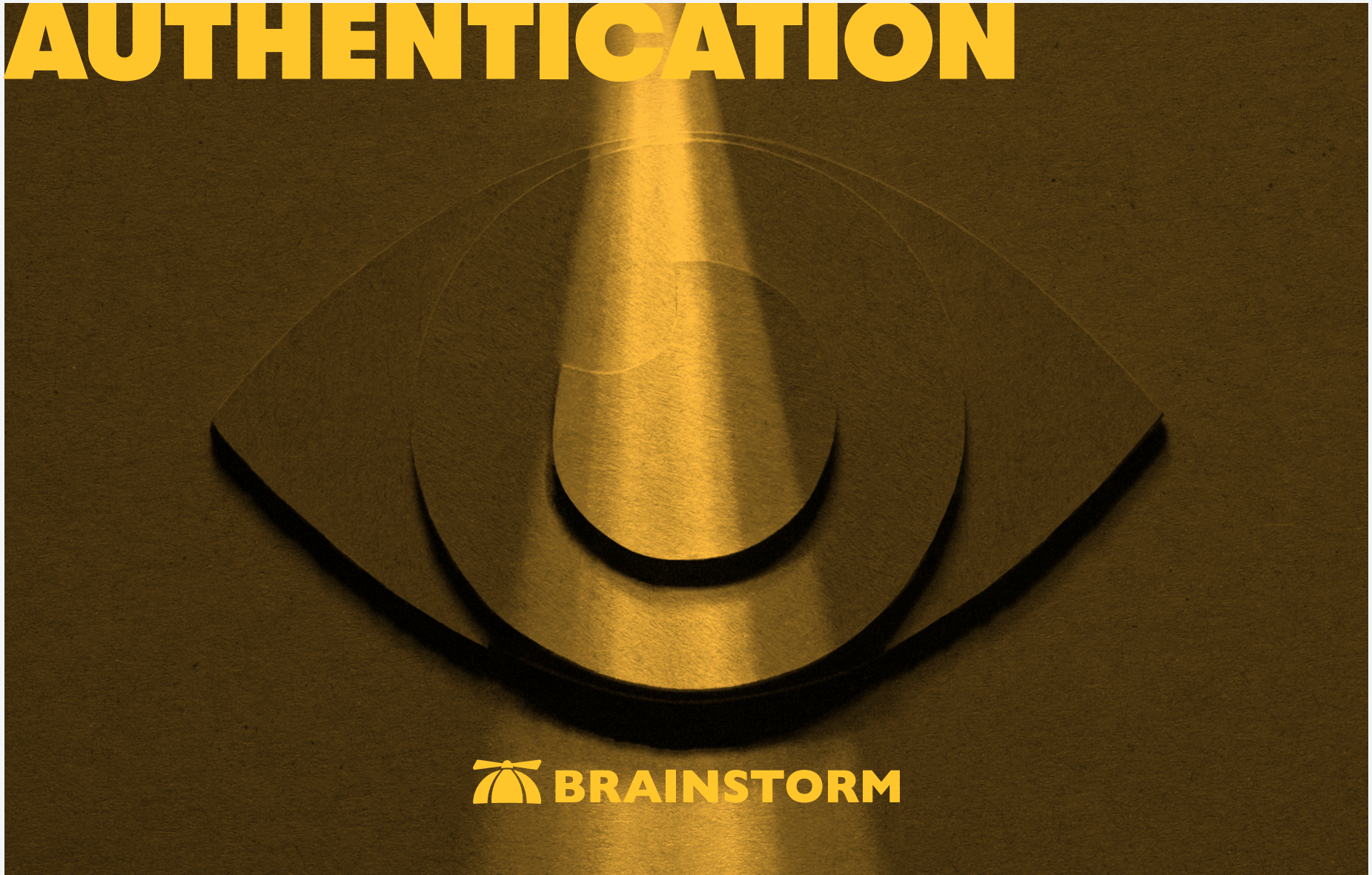
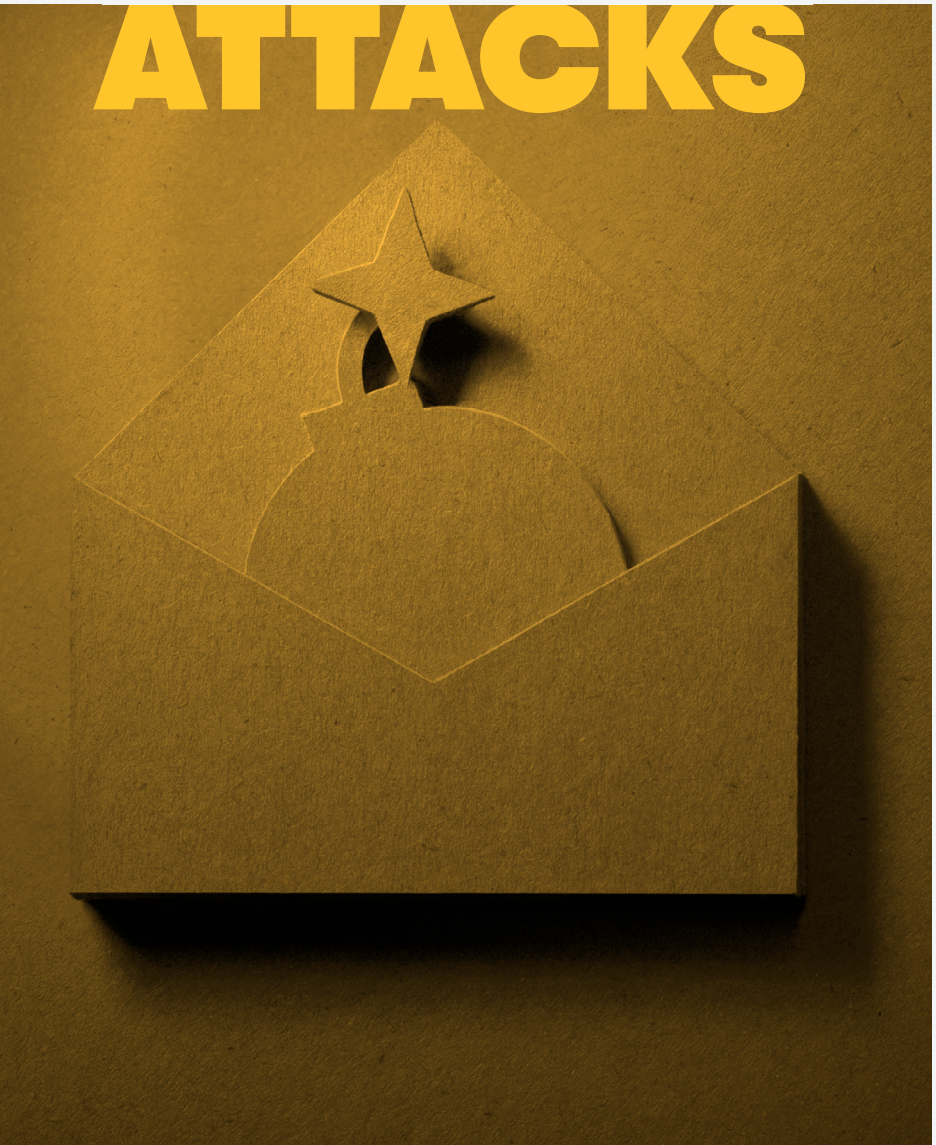
MULTI-FACTOR AUTHENTICATION



THE ONE-TWO PUNCH AGAINST CYBER SECURITY ATTACKS



Multi-Factor Authentication

Still focusing only on password length and strength? It's time to rethink that strategy—because even the best password isn't enough to counteract the worst cyber security threats.

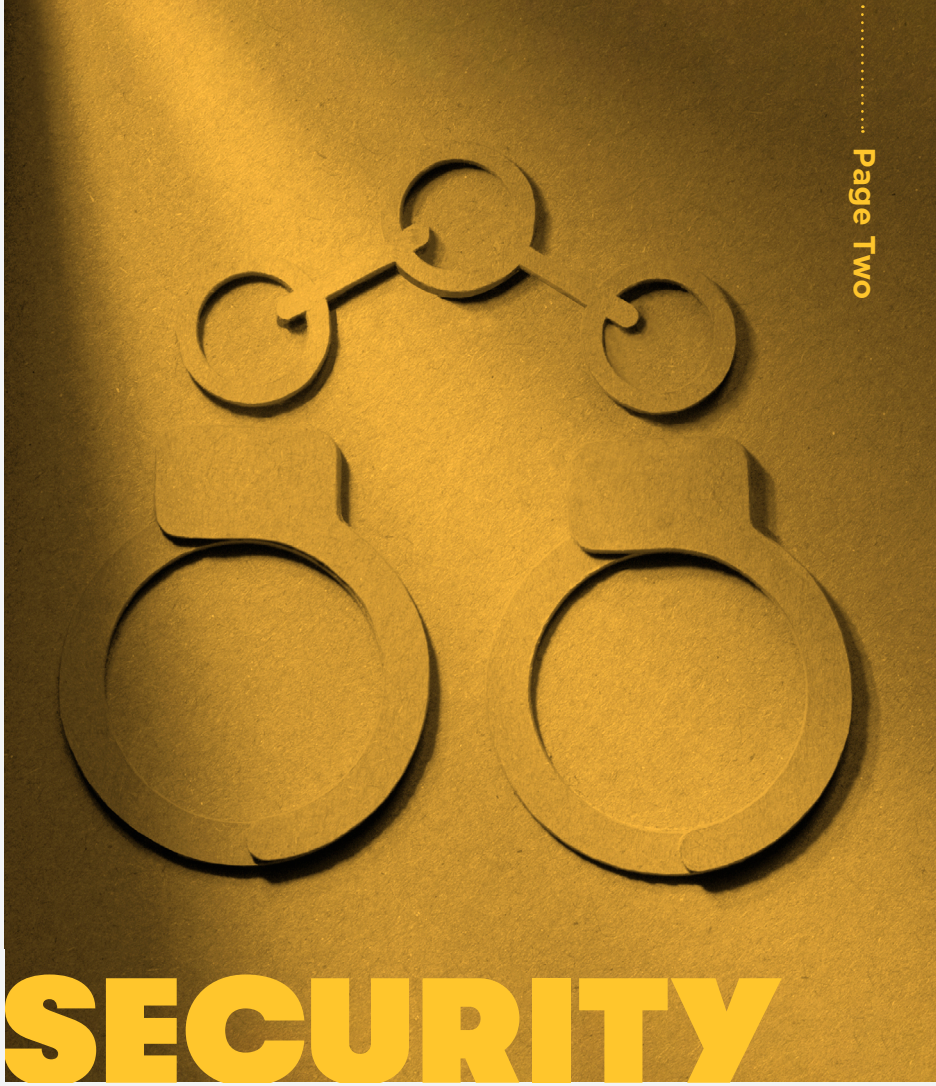
You also should fight back with Multi-Factor Authentication (MFA).

Why Multi-Factor Authentication?

Security breaches are costly, and the expenses can run organizations into the ground. By using your identity and credentials, hackers are taking an easier route to you and your organization's data.

Consider this:

- 81% of security breaches happen because of weak or stolen passwords.[1]
- Only 26% of organizations use multi-factor authentication.[1]
- Multi-factor authentication (MFA) can block over 99.9 percent of account attacks.[2]
- MFA also supports a bring-your-own-device (BYOD) scenario, which is critical to the new world of remote work.



Sources
1. LastPass | 2. Microsoft

OF MFA

MFA — A Common Scenario

Anyone who does online banking already knows about MFA. To log in, an account holder:

1. Enters their password.
2. Receives a random code (usually via text message).
3. Provides that random code to finish logging in.

If a hacker tries to compromise the account holder's password, the second layer of authentication keeps them from being successful.

MFA at Your Organization

If your organization hasn't yet enabled MFA, what should you do?

You've heard the adage that the best time to plant a tree was twenty years ago. The second-best time to plant a tree is today. When it comes to enabling MFA, start where you are now. But start.

MFA at your organization can be done a few different ways, making the process virtually transparent for end users.

For example, many organizations enable multi-factor authorization through certificate-backed smart cards or applications like Microsoft Azure Multi-factor Authentication.[3] While methods may vary, the results are the same.

AVOID THE HIDDEN DANGER

Sources
3. Microsoft Azure

REMEMBER THE HUMAN FACTOR

Educating Your Workforce

Along with MFA, remember the human factor when confronting any data vulnerability.

According to an IBM study[4], human error now accounts for 95 percent of cyber security breaches. That means you'll also need a strategy that helps end users become security savvy.

So, what's the best way to educate users on security best practices? BrainStorm QuickHelp™ can help you scale that message, build new skills, and measure user progress as you enable MFA.

You can do it—and BrainStorm will show you how.

Sources
4. IBM Study

BRAINSTORM

Need a better way to educate users about security? Talk to a BrainStorm change expert.

Get Started

BrainStorm transforms organizations by using technology to empower people and activate change.