

COVER DOWN ON THE BASICS: FOUR ESSENTIALS TO PROTECT YOUR BUSINESS OR GOVERNMENT ORGANIZATION

SECURING
THE NEXT 250

1

TEACH EMPLOYEES TO AVOID **PHISHING SCAMS**



Keep an eye out for phishing and other scam attempts in your emails, texts, direct messages or phone calls. Always verify the sender before clicking links or downloading attachments. If you spot a scam, report it!

2

REQUIRE **STRONG** **PASSWORDS**



All passwords should be:



LONG:

At least 16 characters



RANDOM:

Use a random string of mixed-case letters, numbers and symbols, like:
Yuc8\$RikA34%ZoPPao98t



UNIQUE:

Never reuse passwords

Keep your passwords safe by
using a **PASSWORD MANAGER!**

3

REQUIRE **MULTIFACTOR** **AUTHENTICATION**



Multifactor authentication provides an extra layer of security for your accounts. Choose the most secure MFA method available. A physical security key provides the best protection and is easy to use.

4

UPDATE **SOFTWARE**



Updating software and devices is the easiest way to stay protected from security threats. Perform updates as soon as they become available or set automatic updates.



**CYBERSECURITY
AWARENESS
MONTH**
OCTOBER 2026

cisa.gov/cybersecurity-awareness-month