# 10 CYBERSECURITY TERMS You Need to Know

Cybersecurity can feel like a language all its own. Use this handy guide to decipher some of the more common terms.

## Business Email Compromise [BEC]

A common exploit in which a hacker spoofs an email owner's identity to defraud the company or its employees, customers, or partners.

## Malware

Software that is intended to damage or disable computers, computer systems, and networks.

## Ransomware

A type of malware that prevents or limits users from accessing their system until a ransom is paid.

## Phishing

The use of fraudulent emails to induce individuals to reveal sensitive information like passwords or credit card numbers.

## Two-Factor Authentication [2FA]

A security mechanism that requires two types of credential for authentication—something you have (a PIN you receive by text on your phone) and something you know (your username and password).

## Encryption

A method of encoding information or data to prevent unauthorized access.

## Backups

The process of making additional copies of data in case the original is lost or damaged.

## Anti-Malware

Software that protects against infections caused by many types of malware, including viruses, rootkits, ransomware, and spyware.

## Whitelist

An index of approved software applications that are permitted on a computer system or network.

## SOC 2 Certification

Developed by the American Institute of CPAs (AICPA), SOC 2 defines five "trust service principles" for managing client data—security, availability, processing integrity, confidentiality, and privacy.