



# Benchmarking Campaign

October 2022 • Campaign Overview

**Objective:** Test to see if recipient clicks and logs in

**Domain:** keysaver-registration.com

**Sender:** Benefits Admin

**Subject line:** Profit Sharing Update

Email

To: {email:firstName} {email:lastName}  
From: Benefits  
{emailSendTime:1, F j:America/Chicago}

We are pleased to introduce a new profit sharing benefit currently rolling out that's designed to help you save for the future in times of uncertainty.

Through a partnership with Keysaver, a digital financial innovation firm that's helped millions build wealth through profit sharing programs, we now offer app access to an expanded number of investment funds with proven track records of positive performance.

As an incentive to participate, we're also offering up to a 35% additional match for employees who sign up during the enrollment period that runs through {emailSendTime:1, F j:America/New\_York:+10 days}.

We understand you may have questions about the program, which we've anticipated. The Keysaver link below will take you to a portal that includes a customized Q&A prepared exclusively for our organization.



[click here if Keysaver app icon does not appear](#)

Use your company user ID and password to log in for answers to frequently asked questions and an opportunity to sign up before the deadline to participate passes.

We hope you make the most of this new employee benefit.

Sincerely,  
Your Benefits Team

Login Page



**Sign In**

**User Name**

**Password**

[Sign in](#)

By continuing, you agree to Keysaver's [Conditions of Use](#) and [Privacy Notice](#).

[Need help?](#)

- Campaign is free to Barracuda Security Awareness Training clients providing a company address book.
- Campaign will run October 17 - 21 with data collection through October 28.
- All participants will use the same domain and campaign elements.
- Upon completion, customized reports will be provided to all administrators so they can see how their organization performed and compares to others and industry standards.
- **Sign-up deadline is October 10th.**  
Contact Barracuda Support to sign up.

**YOU'VE BEEN PHISHED!**

The email you just clicked was a test to see how you'd respond. Had this been a real phishing attempt, your actions could have led to a cyberattack!

**LET'S LEARN FROM THIS EXPERIENCE**

Most phishing emails have several traits in common. You can protect yourself and the company by learning to recognize them.

 <p><b>Phony sender</b> Look closely at the sender name. If you don't recognize it or the address, be suspicious.</p>	 <p><b>Recipient issues</b> Large numbers of unrecognizable recipients—or none at all—is a red flag. Be suspicious.</p>	 <p><b>A sense of urgency</b> Requests to act immediately often accompany phishing emails. It's a ploy to make you click.</p>
 <p><b>Dire consequences</b> Threats of negative legal, financial or other actions are typical in phishing emails. Don't be intimidated.</p>	 <p><b>Phony links</b> Hover your mouse over links to see the real web address. If you don't recognize it, don't click.</p>	 <p><b>Appeals to Emotion</b> Emails that play on sensitive life fear, desire, greed and others are often phishing attempts.</p>
 <p><b>Poor Spelling and Grammar</b> Watch for misspellings and errors that are poorly written. These are almost always suspect.</p>	<p><b>REMEMBER, YOU'RE IN CONTROL!</b> If you receive an email that seems suspicious, remember that you're in control. You don't have to act or respond to the email in any way.</p> <p><b>WHAT YOU SHOULD DO</b> Report any suspicious emails to your Information Security team.</p> <p><b>INTERESTED IN LEARNING MORE?</b> Contact your Information Security department for more resources.</p>	<p><b>Please acknowledge you read and understand this information by clicking here.</b></p>

Landing Page