Benchmarking Wrap Up

October 2023

Fall Benchmarking Highlights

Thank you for participating in the Fall 2023 Benchmarking Campaign! This effort was designed to help your organization determine which individuals would click on an authentic looking phishing email.

The email, based on similar phishes identified by Barracuda security tools, mimics one of many effective phishing attacks that use signature requests as a lure. The data highlighted below reflects the combined campaign results:

- **43 organizations participated—a new high.**
- **Nearly 18,000 emails sent.**
- **Average click rate: 13.41%**
- **Median click rate: 8.94%**

In addition, this campaign yielded a wide variety of phishing vulnerability statistics across a several business sectors. We've compiled them into reports you can use to gauge where your organization ranks. You'll find these on the next page.

Although this campaign is over, you can continue to leverage it by using the benchmarking followup materials outlined on the last page of this wrap-up. If you need assistance, please reach out to Barracuda Support.

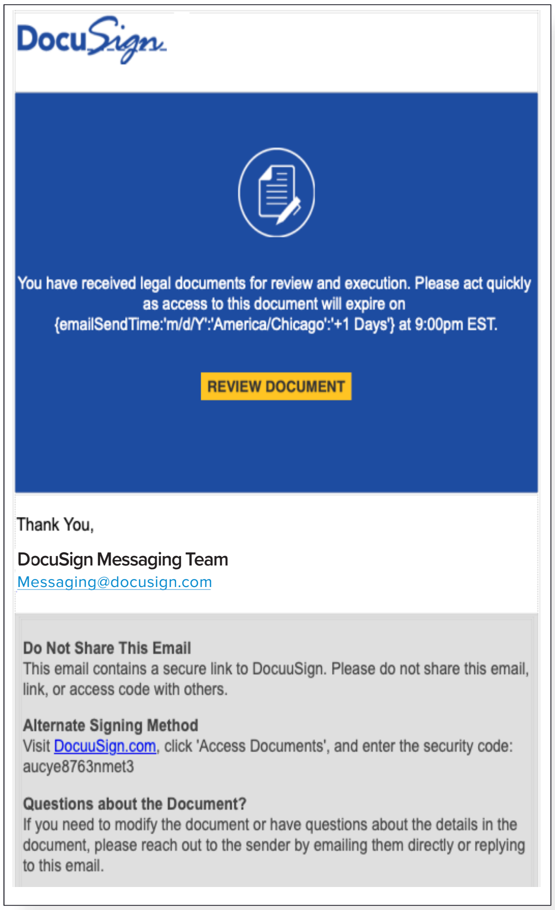
Did you know?

All of our benchmarking campaigns are available for you to run any time. For a comprehensive list, check here and refer to the setup instructions.

The next benchmarking opportunity is in April of 2024. Watch your email and Click Thinking for dates and details.

Campaign Elements

Domain: myofficeaccounts.com
Sender: DocuSign Alert
Subject line: Signature Required



You have received legal documents for review and execution. Please act quickly as access to this document will expire on {emailSendTime:'m/d/Y':'America/Chicago':'+1 Days'} at 9:00pm EST.

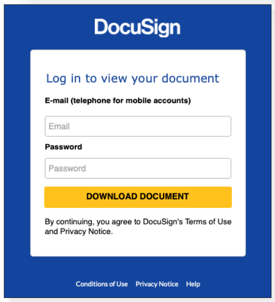
Thank You,

DocuSign Messaging Team
Messaging@docusign.com

Do Not Share This Email
This email contains a secure link to DocuuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuuSign.com, click 'Access Documents', and enter the security code: aucye8763nmet3

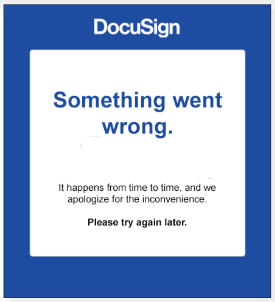
Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.



Log in to view your document

E-mail (telephone for mobile accounts)

By continuing, you agree to DocuSign's Terms of Use and Privacy Notice.



Something went wrong.

It happens from time to time, and we apologize for the inconvenience.

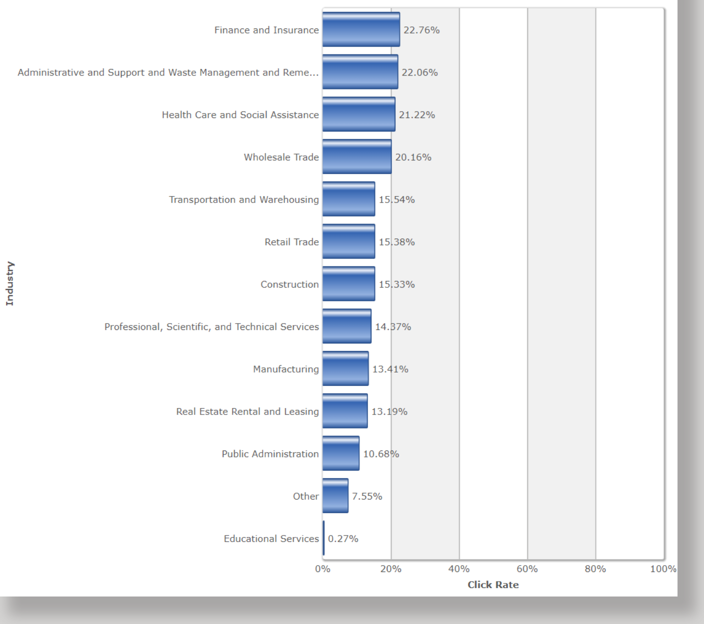
Please try again later.

Benchmarking Analytics

October 2023 Benchmarking Campaign Results — Broken Out By Industry

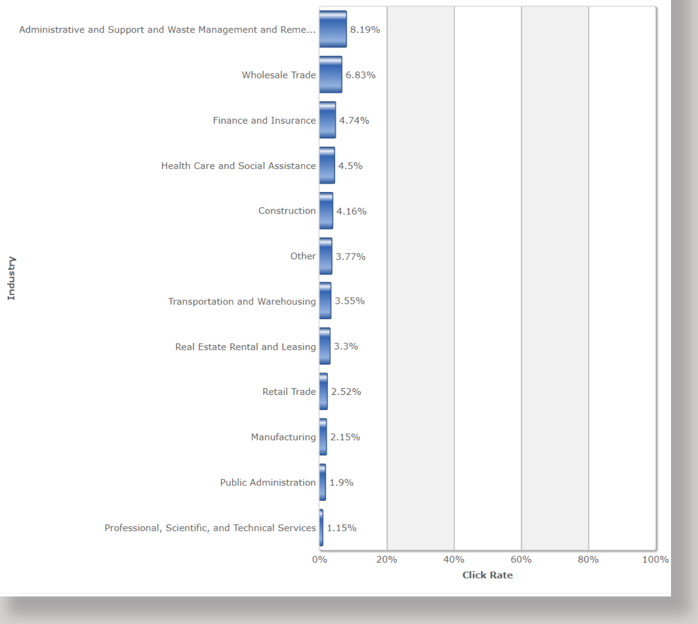
Average Click Rate 13.41%

Individuals who clicked the email



Average Login Rate 3.27%

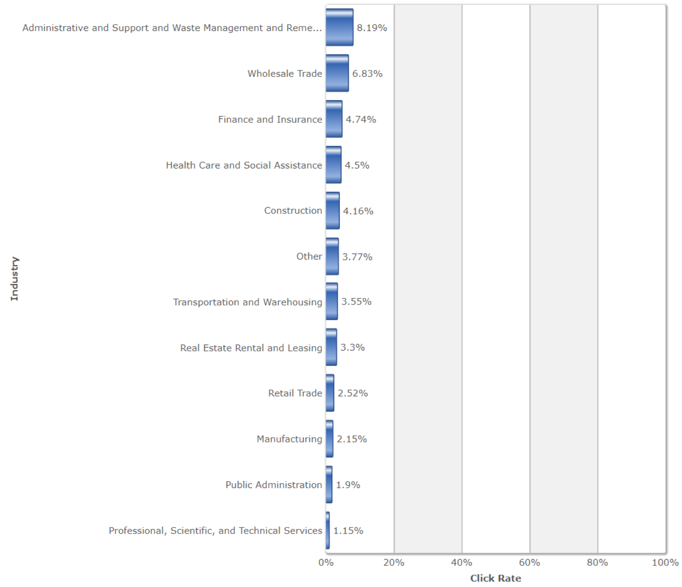
Email clickers who completed the login form



Historical Benchmarking Campaign Results — Broken Out By Industry

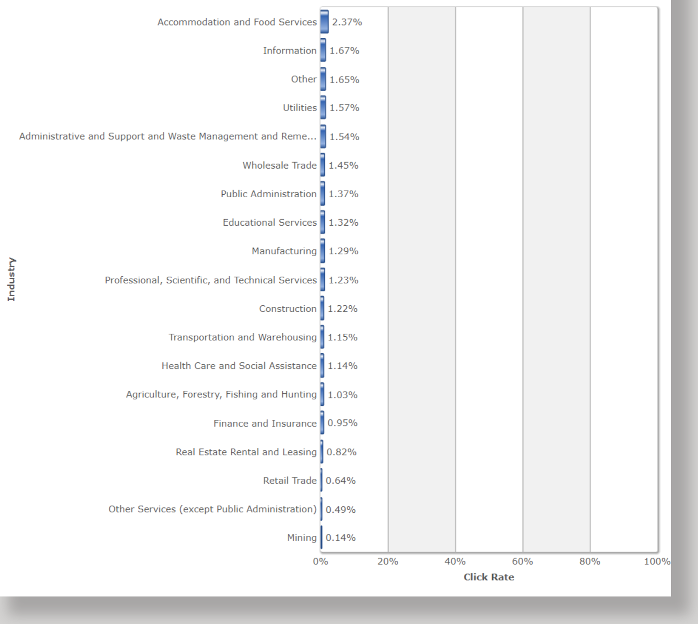
Average Click Rate 9.03%

Individuals who clicked a link in any benchmarking email to date



Average Login Rate 1.18%

Email clickers who completed a login form in any benchmarking campaign to date



You can access these and other benchmarking analytics via the SAT dashboard. Just click the **Results** tab and select **Benchmark Results** from the dropdown menu. For additional insights, visit the benchmarking page on Campus

Benchmarking Followup

The materials below can help you leverage the October 2023 benchmarking campaign and reinforce phishing-awareness concepts. They include emails and a landing page that can be used in a followup campaign and selected training modules. **Search for them by name in the Content Center.**

Hit the Ground Running

For your convenience we've created Content Groups that make followup campaigns easier. One targets those who clicked, the other targets those who didn't. The steps below outline how to deploy them both so you can reach all benchmarking recipients:

- In the **Campaigns** tab dropdown, on the SAT dashboard, click **Campaign Manager**
- click the **+ New** button
- Under the **Testing** heading, click the **Email** option
- In the Campaign Intent dropdown. choose **Testing**
- Give your Campaign a name
- Click the **Enable Content Groups** box
- Click **Save** to be taken to the **General Settings** page
- Under **Scheduling** identify start, end, and cutoff dates
- Under **Targets** select the address book you used for October 2023 benchmarking
- Under targets click **+ Show Advanced Filters**
- Scroll down to **Clicked Link** and select **True** from menu
- Under **Content** click **Add New Content Group** and click **yes** to get to the Content Center
- Use the **Name** filter to search: **2023 10 Benchmark - Training for Clickers**
- Click box and hit refresh
- Click magnifying glass and Click add **Add to My Recent Campaign**
- Click **Go to My Recet Campaign**
- Click the **Save** button
- Review settings and Proceed to **Go Live** stage

This will target clickers who fell for the phish. To target those who didn't repeat the same steps above, but select **False** and **2023 10 Benchmark - Training for Non-Clickers** in the steps highlighted in blue.

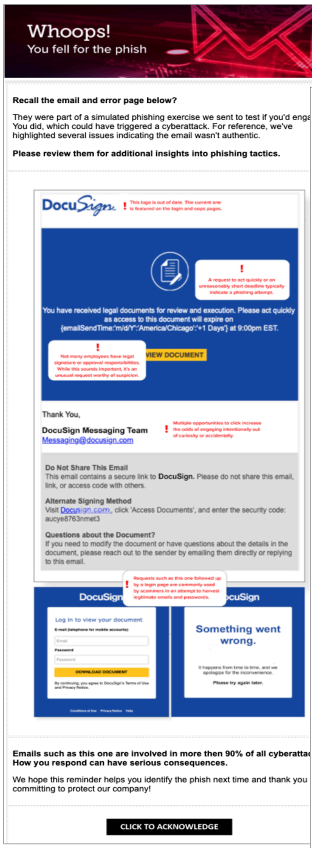
Campaign Building Instructions and Insights

If you're new to campaign building or want to learn more, check out Creating and Generating an Email Campaign on Barracuda Campus. Or click the chat icon located in the lower right corner of the SAT dashboard for tutorials and additional information. In addition, you can alwasy reach out to Barracuda Support if you need further assistance or have questions.

Two emails, one for clickers (negative reinforcement) and one for non-clickers (positive reinforcement):

Email Sender: Barracuda Security Awareness Training
Subject: We tested you with a simulated phishing email. Here's what happened.

Email Title
2023 10 Benchmark - Training for Clickers



Whoops!
You fell for the phish

Recall the email and error page below?

They were part of a simulated phishing exercise we sent to test if you'd enga
You did, which could have triggered a cyberattack. For reference, we've highlighted several issues indicating the email wasn't authentic.

Please review them for additional insights into phishing tactics.

DocuSign ! This logo is out of date. The current one is featured on the login and oops pages.

! A request to act quickly or an unreasonably short deadline typically indicate a phishing attempt.

You have received legal documents for review and execution. Please act quickly as access to this document will expire on {emailSendTime:'m/d/Y':'America/Chicago':'+1 Days'} at 9:00pm EST.

! Not many employees have legal signature or approval responsibilities. While this sounds important, it's an unusual request worthy of suspicion.

VIEW DOCUMENT

Thank You,

DocuSign Messaging Team
Messaging@docusign.com

! Multiple opportunities to click increase the odds of engaging intentionally out of curiosity or accidentally.

Do Not Share This Email
This email contains a secure link to **DocuSign.** Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit Docusign.com, click 'Access Documents', and enter the security code: aucye8763nmet3

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

! Requests such as this one followed up by a login page are commonly used by scammers in an attempt to harvest legitimate emails and passwords.

DocuSign
Log in to view your document
E-mail (telephone for mobile accounts)
Email
Password
Password
DOWNLOAD DOCUMENT
By continuing, you agree to DocuSign's Terms of Use and Privacy Notice.
Conditions of Use Privacy Notice Help

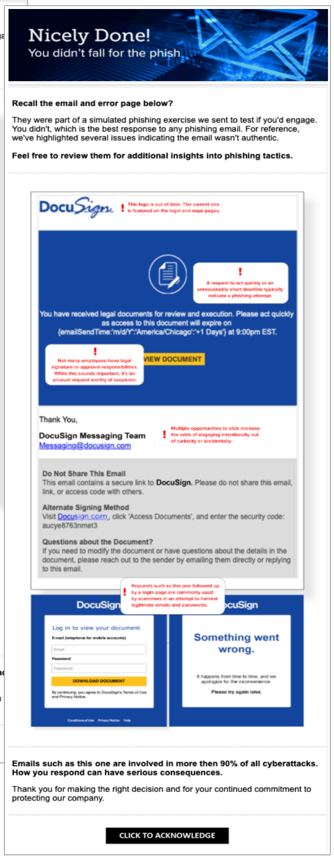
DocuSign
Something went wrong.
It happens from time to time, and we apologize for the inconvenience.
Please try again later.

Emails such as this one are involved in more then 90% of all cyberattac
How you respond can have serious consequences.

We hope this reminder helps you identify the phish next time and thank you
committing to protect our company!

CLICK TO ACKNOWLEDGE

Email Title
2023 10 Benchmarking -
Training for Non-clickers



Nicely Done!
You didn't fall for the phish

Recall the email and error page below?

They were part of a simulated phishing exercise we sent to test if you'd engage. You didn't, which is the best response to any phishing email. For reference, we've highlighted several issues indicating the email wasn't authentic.

Feel free to review them for additional insights into phishing tactics.

DocuSign ! This logo is out of date. The current one is featured on the login and oops pages.

! A request to act quickly or an unreasonably short deadline typically indicate a phishing attempt.

You have received legal documents for review and execution. Please act quickly as access to this document will expire on {emailSendTime:'m/d/Y':'America/Chicago':'+1 Days'} at 9:00pm EST.

! Not many employees have legal signature or approval responsibilities. While this sounds important, it's an unusual request worthy of suspicion.

VIEW DOCUMENT

Thank You,

DocuSign Messaging Team
Messaging@docusign.com

! Multiple opportunities to click increase the odds of engaging intentionally out of curiosity or accidentally.

Do Not Share This Email
This email contains a secure link to **DocuSign.** Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit Docusign.com, click 'Access Documents', and enter the security code: aucye8763nmet3

Questions about the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly or replying to this email.

! Requests such as this one followed up by a login page are commonly used by scammers in an attempt to harvest legitimate emails and passwords.

DocuSign
Log in to view your document
E-mail (telephone for mobile accounts)
Email
Password
Password
DOWNLOAD DOCUMENT
By continuing, you agree to DocuSign's Terms of Use and Privacy Notice.
Conditions of Use Privacy Notice Help

DocuSign
Something went wrong.
It happens from time to time, and we apologize for the inconvenience.
Please try again later.

Emails such as this one are involved in more then 90% of all cyberattacks.
How you respond can have serious consequences.

Thank you for making the right decision and for your continued commitment to protecting our company.

CLICK TO ACKNOWLEDGE

A common landing page

Landing Page Title
2023 10 Benchmarking LP

A unique ghost landing page that opens and closes to register the "Click to Acknowledge" completes this follow-up campaign.

It has no content and appears so quickly users are unlikely to notice.

Additional training modules:

These modules are also recommended for additional followup:

- Phishing Signs Click Thinking Express (Title: CTE-1)
- What is Phishing With Quiz (Title: P101A-1)
- Phishing Awareness Click Thinking Interactive Training (Title: CTI-1)