BioCatch

SOLUTION BRIEF

Lookalike Site Alerts in Real Time

With 24hr Victim Reports informing you which of your customers has been fooled into sharing their sensitive data.

Phishing Sites Explained

A phishing site is a domain similar in name and appearance to an official website. Its purpose is to pose as a legitimate institution and lure individuals into providing sensitive data such as PII, banking details and passwords. When fraudsters obtain this sensitive data, it can lead to much bigger problems down the line such as account takeover and social engineering scams.

This is what a lot of organizations don't realize, phishing sites are just the beginning. They form just one key component of a wider banking fraud framework.

Our Phishing Site Detection Solutions

Real Time Alerts

Lookalike phishing site alerts in real time straight to your inbox

Next-Day Reporting

Lookalike phishing site alerts sent to your inbox every 24hrs

Key Benefits

Victim Reports: Get a list of the customers who have been fooled into sharing their sensitive data

Reduce the cost of more sophisticated fraud happening further down the line

Protect company reputation and help prevent customer data from falling into the wrong hands

Sustain and increase trust levels with existing and new customers

A Problem That Is Not Going Away

Although the profile of phishing sites has been significantly raised over time, attackers are still finding new and innovative ways to fool users into believing their actions involve a legitimate website, email, phone call or text.

The impact of a successful phishing attack on an organization can be catastrophic. Their reputation can be permanently tarnished resulting in existing customers leaving and new customers not joining.

Fighting Fraud Downstream

Phishing is often just the starting point for criminals in the attack lifecycle. The real risk isn't introduced until stolen credentials are used to initiate a fraudulent payment or transaction. In studying the downstream impact of known users that visited a rogue phishing site, BioCatch data reveals in the first 14 days:

Two Options to Combat Lookalike Phishing Sites

Our two phishing site detection solutions can help you reduce fraud costs, protect your customers from a negative experience and reduce the number of operational hours spent resolving and processing cases of fraud.

BioCatch believes that acting quickly upon discovering a phishing site is key to preventing other types of fraud further down the line. Therefore, both of our phishing solutions can be provided with Victim Reports, informing you which of your customers has been fooled into sharing their sensitive data.

Real Time Alerts (Recommended)

Lookalike Phishing Site Alerts in Real Time Straight to Your Inbox

Customers are alerted in real time via email about new lookalike phishing sites

The fraud window of opportunity is even smaller than next-day reporting, minimizing the window of opportunity for the theft of sensitive data

or

Next-Day Reports

Lookalike Phishing Site Alerts Sent to Your Inbox Every 24hrs

Daily alerts are sent to customers every 24 hrs to a designated contact and at a designated time

HIGH traffic phishing sites are highlighted and marked for urgent action

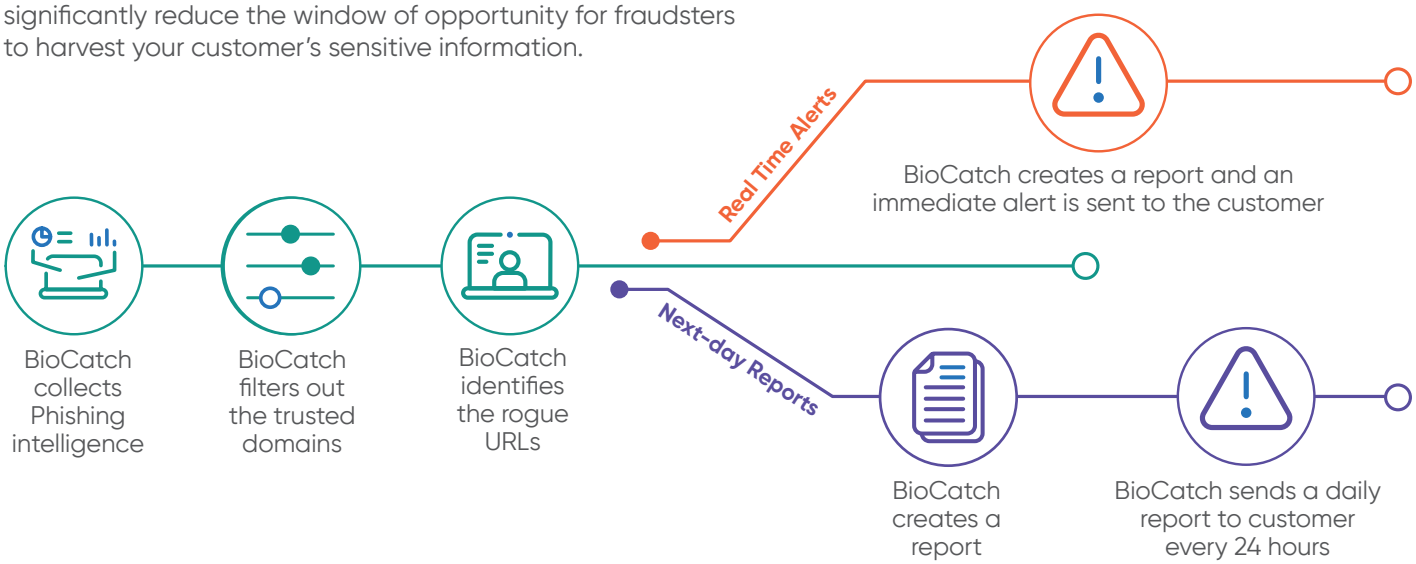
+

Victim Reports

Get a list of customers identified via their UID so you know who has been fooled into sharing their sensitive data

How Our Solutions Work

Both our Real Time Alerts and Next Day Report solutions significantly reduce the window of opportunity for fraudsters to harvest your customer's sensitive information.



Combat Phishing And Other Types Of Social Engineering With Behavioral Biometrics

The emergence and takedown of phishing sites will unfortunately be an endless reoccurring cycle. Despite having effective phishing solutions in place, personal information of customers will continue to slip through net and fall into the wrong hands. Behavioral biometrics detects when fraudsters try to use stolen information by monitoring HOW information is entered, not WHAT is entered.

Behavioral Biometrics VS Conventional Fraud Detection Solutions

Example 1: Credential Stuffing and Harvesting

In a credential or personal information harvesting attack, a fraudster steals login credentials and uses them to log into a victim's account. Conventional fraud detection methods are unable to detect that it's a fraudster using the account because the login authentication is correct. Behavioral insights, however, detect when a user's credentials have been compromised by evaluating how the user acts after they log in. If the actions do not match the normal behaviors of that account user, behavioral analysis detects the difference in cadence and rhythm and flags the session as potentially compromised by a fraudster.

Example 2: SMSishing

For SMShing, fraudsters may trick an individual into handing over a strong authentication code used in two-factor authentication. Once again, unlike conventional fraud detection solutions behavioral analysis can detect a fraudulent account session by monitoring how information is entered after login and offers continuous real time protection.

Example 3: Vishing

It works the same for scams that involve a victim taking instruction from a fraudster over the phone. In this scenario, the victim is prompted to take action or enter information, meaning they may take longer to enter information on a page than normal, or they may enter information in an unusual pattern. Behavioral analysis can reveal these variances and raises an alert that a customer may be unknowingly partaking in a social engineering scam.

Find out more, contact BioCatch

The best way to combat all these types of attacks is to build behavioral biometrics into your fraud prevention stack and not just rely on static identifiers. Contact BioCatch for further information.

www.biocatch.com E: info@biocatch.com @biocatch /company/biocatch

BioCatch is the leader in Behavioral Biometrics which analyzes an online user's physical and cognitive digital behavior to protect individuals and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of analyzing data, over 60 patents and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems. For more information, please visit www.biocatch.com

Tel Aviv | New York | Boston | London | São Paulo | Santiago | Mexico City | Melbourne | Mumbai | Singapore