SOCIAL MEDIA COVERAGE

MONARCH NATIONAL

DESCRIPTION

Social Media Coverage is a service that closes five fundamental gaps left wide open by the social networks.

1. First, Social Media Coverage identifies all social network accounts in the public domain that share the policyholder's username, nicknames, and profile image so that the policyholder can easily determine what social network accounts belong to them and what social network accounts are impersonating them.

2. Second, Social Media Coverage informs the policyholder when personal information is inadvertently or deliberately exposed on the social network platform.

3. Third, Social Media Coverage keeps track of incoming and outgoing posts/mentions that reference inappropriate language — emoji too — and references to illicit activity, drugs and violence.

4. Fourth, Social Media Coverage protects policyholders from a persistent but growing threat of phishing and malware attacks. Social networks are a growing platform on which perpetrators launch phishing and malware scams, and Social Media coverage alerts members when one of these harmful links is present on their profile, newsfeed, or timeline.

5. The fifth, and most critical gap that Social Media Coverage closes, is providing the policyholder actionable remediation options that are embedded in every alert. Policyholders can delete or hide offensive and harmful content, and in extreme cases request the offending content or account be removed from the social network platform. Behind the scenes is a robust platform that utilizes machine learning technology that continually learns from policyholders input and tunes the alert rules to provide more precise, accurate, and timely alerts. Furthermore, machine-learning technology is leveraged to spot anomalies with a policyholders expected social network patterns, which can be a leading indicator that a policyholder's account has been hijacked.

FEATURES AND BENEFITS

Protect All Your Personal/Family Policyholder's Accounts

- Protect an unlimited number of personal accounts on Facebook, Twitter, LinkedIn, Instagram and YouTube. Easy activation and dashboard view makes it easy to stay on top of all your social media activity.

Take Action Across All Major Social Networks

- Delete, block user, and takedown offending content on Facebook, Twitter, LinkedIn, Instagram and YouTube.
- Detects known fraudulent links including scam and phishing links that are associated with your protected profiles.
- Block, takedown or un-tag your profiles from malicious links from one easy to use dashboard.
- Takedown impersonating profiles.
- Scans social networks for accounts that may be using the name and profile photos of your protected accounts. If found, you'll have the ability to start takedown procedures of the impersonating account so that others can't hijack your reputation.
- Remove inappropriate content.
- Delete or hide offensive and harmful content that risks degrading your reputation.

Scan the Dark Web for Compromised Credentials

- The first step to protecting your social media is making sure your credentials are secure. We'll alert you if your credentials are for sale on the dark web or if they were compromised in a past data breach.

Get Alerted to PII Exposure

- One of the most common ways to become a victim of identity theft is inadvertent PII exposure. Easily identify when PII has been posted so that you can delete or remove from public view.

Identifies Thousands of "Threat Triggers"

- A growing knowledge base of intelligence on the latest threats and scams ensures Social Media coverage protection stays on the cutting edge of social media privacy and fraud threats.

Advanced Technology like Artificial Intelligence and Machine Learning to meet Evolving Threats.

- Social Media Coverage is always learning about new scams and threats as well as activity anomalous to your specific social media account.

ANTICIPATED QUESTIONS FROM POLICYHOLDERS

Is my information secure?

Yes. As a leading identity protection service provider, we take information security very seriously. We've taken painstaking measures to ensure your data is protected, hashed, and encrypted, even when we need to communicate with our trusted data partners.

Is my information ever sold or provided to another third party who might contact me with promotional offers?

No. As a policyholder, we see you as a valued customer, not a product.

What social networks do you monitor?

We monitor Facebook, Instagram, Twitter, LinkedIn, and YouTube. We also monitor Paste Bins and P2P sharing sites for the presence of your social media login credentials.

Why do I need to connect my social network accounts?

In order for us to provide our monitoring service to you, we require access to certain areas of your social network account, like your profile picture, user name, and timeline/newsfeed. Access to this data allows us to identify when someone is impersonating you, leaking your personal information, damaging your reputation, or tricking you into their latest scam. Furthermore, allowing us access to your social network account gives us a unique ability to remediate any offending content directly from within our alerts.

What triggers an alert?

In general, there are five scenarios in which an alert can be generated. The first is if we detect another account with the same username and profile image (which we refer to as (impersonation). Second is if we detect your personal information in a post. Third is if we detect someone posting content that is potentially damaging to your reputation. Fourth, we detect anomalous profile activity, for example, a sudden change to your profile picture or username. Finally, we detect if someone posted content that contains a known malicious link that either installs malware or takes you to a phishing website.

What do the buttons in the alert do?

- Report user: Automatically opens a case with the social network asking them to investigate the reported content and the user who authored the content. If any violations to the social network's terms of service are violated, the social network can take steps to remove the content. In some circumstances, the author of the offending content can also be suspended or removed from the social network platform. This feature applies to all monitored social networks.
- Block user: Results in the user being blocked from tweeting, @mentioning you, or sending direct messages to your account. Additionally, any tweets from the blocked user's account are hidden from your account. This feature only applies to monitored Twitter accounts.
- Hide content: Results in the tweet, @mention, or direct message being hidden from view on your account. This feature only applies to monitored Twitter accounts.
- Archive: Sends the alert to your archive so you can revisit it later.

Why was my request to report a user denied?

Acceptance of your request to remove content or a user is subject to each social network's terms of service agreements and each circumstance has a probability of being accepted. Probabilities are based on our past experience in dealing with these issues. In general, content that contains nudity, hate speech, disclosure of personal identifiable information, or malicious links has a high probability of removal. In cases where the removal request is denied by the social network, we provide a direct link to the offending content where you can access additional tools on the social network to remove, block, or hide the offending content.

Can I make additional removal requests?

You are only allowed one removal request per alert.

What words or phrases will trigger an alert?

We maintain a vast library containing thousands of words and phrases that we continue to develop. This library of words and phrases also contains variants and alternative spellings so we can catch instances of trickery or attempts to outsmart our alert triggers. Policyholders can suggest or request additions to our growing list of words and phases.