

CASE STUDY

Automattic: Automating the process of detecting account exposures and protecting the account from a takeover.

CHALLENGE

Password reuse is a constant issue that often leads to account takeovers, yet finding exposed credentials was a labor-intensive, manual task that didn't capture every instance.

SOLUTION

Automattic chose SpyCloud to automate the process of detecting account exposures and protecting customer accounts from a takeover with proactive tools that force an immediate password reset.

RESULT

With the automated solution, Automattic is protecting millions of people from account takeover and preventing them from reusing exposed passwords for a safer customer experience.

HOW AUTOMATTIC IS PROTECTING CUSTOMERS BEHIND THE SCENES

Automattic is the company behind one of the most popular online publishing platforms in the world, WordPress.com. WordPress.com is but one of the products offered by Automattic. The company has developed services like Jetpack and WooCommerce that give users additional functionalities such as ecommerce, website security, backups and anti-spam capabilities. With a motto of "making the web a better place," clearly Automattic is defining how the internet can empower, inspire and delight.

Today, customer accounts have become a target for cybercriminals who seek to hack accounts to steal identities, data or privileges using stolen credentials. When people reuse passwords across multiple sites and apps, they make themselves highly vulnerable to attacks. Automattic took up the cause to ensure its customers were as secure as its own servers, offering multi-factor authentication and ensuring customers choose strong passwords that have never been exposed on the dark web.

ENHANCING THE WEBSITE EXPERIENCE

Automattic's mission is to give people easy access to a platform where they can share data beyond social media accounts. "We believe everyone should have their own place on the web, their own domain they own forever," says Barry Abrahamson, CTO at Automattic. "While affordable, we give them inventive tools to make it unique, interactive and highly functional."

What was once primarily a blogger's paradise, WordPress.com has expanded to give businesses of all sizes across the globe a place to connect with an audience in ways never before possible. "Protecting our customers from account takeover is something we view as our responsibility," says Abrahamson. "Many people

may not realize the risk of reusing passwords across multiple accounts. Our goal is to both educate our users and protect their WordPress.com site as much as we can from all forms of attacks. We do all of the work behind the scenes so customers can just enjoy their site and the freedom it brings to express themselves."

Automattic is unique. They don't charge extra for the many security features embedded in their products. Everything is included in the platform because the company believes at its core that those features are too important to leave to chance. A

“

Protecting our customers from account takeover is something we view as our responsibility... Many people may not realize the risk of reusing passwords across multiple accounts. Our goal is to both educate our users and protect their WordPress.com site as much as we can from all forms of attacks. We do all of the work behind the scenes so customers can just enjoy their site.



secure presence on the internet is a basic right, not an opportunity to nickel and dime customers. To Automattic, Denial of Service, SSL, web application firewalls and account takeover prevention are features as important as any basic product functionality, maybe more.

“Our idea behind security is to provide best-in-class security features and functionality to all customers in a transparent, no-hassle way, whether they ask for it or are completely oblivious to its necessity,” says Abrahamson. “We ensure when we implement something, we make the default version as secure as technically possible. Security features are automatically enabled, without requiring the user to turn on a feature, so we know our customers are protected from bad people who want to cause harm.”

PROACTIVELY PREVENTING ACCOUNT TAKEOVER

Account takeover has come front and center in the past few years. According to Verizon, stolen credentials top the list of breach attacks, mostly due to the fact that nearly 60 percent of people admit to reusing passwords across multiple accounts. Automattic believes it can be more effective in protecting its millions of customers by embedding security solutions into its products.

One such solution Automattic chose was SpyCloud to automate the process of detecting account exposures and protecting the account from a takeover with proactive tools that force an immediate password reset. “Account compromise due to password reuse has become a larger problem over the years,” says Abrahamson. “We found ourselves spending more of our time searching the dark web for these password lists and then going through manually comparing the list with our customer list, then proactively resetting their passwords. It was a huge time commitment. Now that we have an automated solution, we can protect

hundreds of millions of people and prevent them from choosing passwords that have already been exposed.”

Plenty has changed since Automattic was founded, yet the company has the foundation in place to stay nimble to whatever comes next. Automattic continues to build tooling and algorithms internally that detect, block, alert and notify. “We will invest in security measures that are proven to bring value to our products by providing a safe environment for our customers,” he says. “Security will always be at the top of our priority list because it’s our responsibility to take care of our customers who trust us.”

“

Now that we have [SpyCloud], we can protect hundreds of millions of people and prevent them from choosing passwords that have already been exposed.

About Barry Abrahamson

Chief Technology Officer may be on Barry Abrahamson’s resume, but Automattic insiders prefer to call him Systems Wrangler. Abrahamson knows technology. He was one of the original hires at Automattic and for more than 12 years, has worn plenty of hats. He is responsible for all of the technology and implementations at Automattic, including servers, data centers and security, as well as improving performance and security insights. Before joining Automattic, Abrahamson was a senior account manager at Rackspace Managed Hosting.

