

Recovery Unplugged



Challenges

- Phishing attacks are becoming increasingly sophisticated
- High-value medical data frequently targeted by hackers
- A lean and overtaxed cybersecurity team

Solution

- IRONSCALES' AI-powered anti-phishing solution
- Phishing simulations and awareness exercises through IRONSCALES' educational tool

Results (Jan 1 – May 10, 2022)

- 4,070,612 emails inspected
- 29,760 emails remediated
- 572 resolved phishing incidents
- 430 hours and 42 minutes of analyst time saved

Company Intro

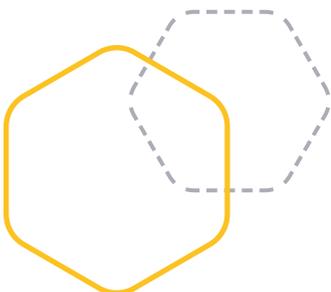
Recovery Unplugged is a US-based addiction treatment organization with seven facilities across Florida, Texas, Virginia, and Tennessee. Providing a variety of rehabilitation services, including detox, residential, and outpatient, the organization is the first addiction treatment provider to run a music program alongside traditional therapy. With a mission to help clients use music to restore hope and healing, Recovery Unplugged has treated over 8,000 clients and has an employee base of over 400 staff.

The Problem

Stolen medical records are worth 50 times as much as financial data on the black market, making healthcare organizations some of the most high-value targets for phishing attacks. And with phishing attempts not just increasing but consistently evolving in sophistication, malicious emails are becoming harder to detect for both users and native inbox filters. Concerned about their clients' high-value medical and financial data, the Recovery Unplugged team was alarmed to see a recent sharp increase in advanced spoofing emails targeting their HR team and C-Suite.

“Long gone are the days of in-your-face, easy-to-spot phishing messages. They’ve gotten so sophisticated that if you’re not using a multi-layered approach, you’re behind. And we can’t afford to be a single step behind.”
 – Jonathan Kaye, Director of IT at Recovery Unplugged

The social stigma surrounding substance abuse means that any breach that exposes clients' medical history, financial information, or treatment details could cause huge damage to clients' personal lives and their progress within the program, as well as to the organization's reputation. And with a lean security team, Recovery Unplugged found the inspection and remediation of malicious emails for over 400 employees to be overwhelming for their lean IT staff, which is also responsible for ensuring that the organization was always in compliance with regulatory standards like HIPAA and PCI DSS.





“What we noticed here was that the majority of our issues were internal. Whether it’s a lack of end-user training and education or general unfamiliarity with scrutinizing emails, we knew that we needed to start with our employees. We needed our user base to be our first line of defense.”

JONATHAN KAYE, DIRECTOR OF IT AT RECOVERY UNPLUGGED

Solution

The security staff needed a solution that could detect and remediate phishing threats automatically, with minimal input from their internal team. Recovery Unplugged felt that it was important to strike the right balance between strong security and manageable cost, with an aim to keep IT overhead as low as possible. Recovery Unplugged’s vendor partner Sirius, a CDW company, recommended IRONSCALES after seeing its success with other clients and overall ease of use. After a short discovery process, the Recovery Unplugged team was able to get the full IRONSCALES solution installed across 400 users within an hour.

“The implementation process was very straightforward. Within an hour it was up and running, and there were very few actions needed after installation. Any questions we had, IRONSCALES answered quickly and easily.”

- Jonathan Kaye, Director of IT at Recovery Unplugged

Outcomes

Immediately after implementation, IRONSCALES began automatically remediating emails and using AI to continuously learn from emails reported by end-users. Between January 1st and May 10th of 2022, IRONSCALES inspected over four million of Recovery Unplugged’s emails, remediating over 29,000 threats and resolving 572 phishing incidents. This amounts to around 430 hours (over 3 hours per day!) of remediation time saved, allowing the busy security team to focus on other important tasks. Recovery Unplugged is now able to automatically remove malicious emails from user inboxes at scale and at the click of a button, affording them greater peace of mind.



“The automated remediation takes a lot of work off my plate in terms of remediating threats and detecting which users have been hit. With over 400 users, plus multiple other shared mailboxes, remediating threats alone could be a full-time job.” - Jonathan Kaye, Director of IT at Recovery Unplugged

Recovery Unplugged’s security team has found IRONSCALES’ easy-to-use dashboard particularly valuable, giving them increased visibility across their email incidents and user base. And being a part of the IRONSCALES Community means that common and emerging threats targeting other organizations can be identified, communicated, and prevented. The team has noticed a significant reduction in spoofing and other email threats, including those targeting HR and C-Suite employees, putting the business in a better position to ensure compliance with the relevant industry standards.

“Whatever cost email security comes to, it’s certainly a lot less than if we had to pay out for a compliance issue, a HIPAA lawsuit, or if we needed to contract a third party to conduct a forensic analysis after a breach.”

JONATHAN KAYE, DIRECTOR OF IT AT RECOVERY UNPLUGGED

Recovery Unplugged has also leveraged IRONSCALES’ fully integrated training and phishing simulation capabilities, using the pre-packaged templates to mimic various malicious email scenarios, including password change requests and W-2 scams during tax season. Through the dashboard, the security team is then able to see who is clicking on these links and who are entering personal details, helping to further tailor campaigns to specific users or departments. Recovery Unplugged has seen a dramatic improvement in phishing awareness since running these campaigns, with increasingly targeted campaigns being sent out as the staff base improves.



I would absolutely recommend IRONSCALES – it’s a great price point and has been working really well for our 400+ staff. We’re based across multiple states and facilities, so its ease of implementation and management alone makes it the best option for us.”

JONATHAN KAYE, DIRECTOR OF IT AT RECOVERY UNPLUGGED

Looking Ahead

The security team at Recovery Unplugged is looking forward to increasing the use of IRONSCALES as the business and staff base grows, as well as continuing to run phishing simulations with an aim to prevent potential phishing incidents. Recovery Unplugged is looking to build phishing awareness education into their onboarding processes and future learning management system.

“I would absolutely recommend IRONSCALES – it’s a great price point and has been working really well for our 400+ staff. We’re based across multiple states and facilities, so its ease of implementation and management alone makes it the best option for us. - Jonathan Kaye, Director of IT at Recovery Unplugged

About IRONSCALES

Every day criminals launch billions of new phishing attacks. No company is immune. Legacy solutions can’t keep up & cloud providers struggle to stop advanced attacks with native controls. IRONSCALES’ powerfully simple email security solution helps you fight back fast and keeps your company safe in today’s cloud-first world.

Incubated inside the world’s top venture program for cybersecurity and founded by alumni of the Israeli Defense Forces’ elite Intelligence Technology unit, we offer security professionals an AI-driven, self-learning email security platform that provides a comprehensive solution to proactively fight phishing attacks.

To learn more about IRONSCALES’ award-winning anti-phishing solution, please sign up for a demo today at <https://ironscales.com/get-a-demo/>

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com   



Learn how working with IRONSCALES makes us Safer Together. www.ironscales.com

Everything is just a click away, from initial installation to threat identification and removal.