MAIL.RU GROUP HITS $1,000,000 IN BOUNTIES

Mail.ru Group came early to bug bounty. After six years with the HackerOne community, the company has uncovered and fixed 3,400+ vulnerabilities and has grown the program into one of the largest and most respected in the world.

mail.ru group | hackerone

The Mail.ru Group security team was early to adopt bug bounty. Since the program launched in 2014, the company has received 3,465 valid reports, including 83 critical and 234 high severity vulnerabilities. Now, as the team sets its sights on even bigger things, the program has hit a huge milestone: **over $1 million paid in bounties.**

To celebrate, we sat down with Vladimir Dubrovin, Information Security Technical Advisor at Mail.ru Group to talk about the lessons he's learned from six years of bug bounty.

During the interview, Vladimir explained why Mail.ru Group got started with bug bounty, tactics used to grow and promote the program, and what's coming next.

KEY STATS

PRODUCT TYPE

HackerOne Bounty

LAUNCH DATE

2014

TOTAL BOUNTIES PAID

>$1M+

UNIQUE HACKERS

999+

VULNERABILITIES RESOLVED

3,409+

RANK FOR MOST VULNERABILITIES SOLVED IN A PUBLIC PROGRAM

#3

HIGHEST BOUNTY

$35K

WHY BUG BOUNTY?

Mail.ru Group got into bug bounty for one reason: to eliminate as many critical vulnerabilities as possible. Since the program launched, Mail.ru Group has paid out hundreds of thousands of dollars for critical vulnerabilities reports, a fact that Vladimir Dubrovin is proud of.

"We started our journey with bug bounty because it's a way to find critical vulnerabilities that other security processes miss. If we're finding those critical vulnerabilities, we know our cybersecurity strategy is effective," he explains.

> **"If our bug bounty program can find at least one critical vulnerability per quarter for two or three quarters in a row, we know the program is worth the money we spend on it."**
>
> **VLADIMIR DUBROVIN**
>
> **INFORMATION SECURITY TECHNICAL ADVISOR, MAIL.RU GROUP**

HOW HAS THE PROGRAM EVOLVED?

When the program first launched in 2014, it focused on identifying critical vulnerabilities such as RCE, SQL injection, XSS, and directory traversal. Only the company's Mail, Cloud, and Calendar services were in scope, and even critical vulnerabilities in other services were excluded. The decision was a practical one — almost every account across Mail.ru Group's services was bound to an email account, so those core services were most important from a security standpoint.

However, since the beginning, Mail.ru Group made the decision to pay out even for issues that were technically out of scope. Vladimir explains why: It's not worth building a fence if it can be bypassed just two steps to the side. Now we cover every high severity issue that belongs to Mail.ru Group, with no exclusions.

Over time, more and more services have been added to the program, and the company has taken radical steps to promote the security of its services.

"We also have an uncommon rule in our bug bounty program." He continued. "We officially pay bounties for reports of our partners' vulnerabilities. When we make agreements with new partner services, we include in the contract that the service must be ready to be bug hunted by hackers and have an SLA in place for fixing security issues.

> **"I've heard this is not so easy to do in other countries due to legal issues, but we want partners to be as secure as we are, so we accept those bugs into our bug bounty program and pay out for them."**

HOW MAIL.RU GROUP INCENTIVIZES HACKERS

As a central component of the company's security program, Mail.ru Group takes bug bounty seriously. That means learning from experience and finding the best ways to engage with the HackerOne community.

So how do you bring the best out of hackers? Vladimir recommends offering creative incentives. For example, the company has offered grants for top hackers, where they are paid for their work whether or not they find a bug. This helps to keep them engaged with the program and motivates them to look for bugs in areas that might otherwise be skipped.

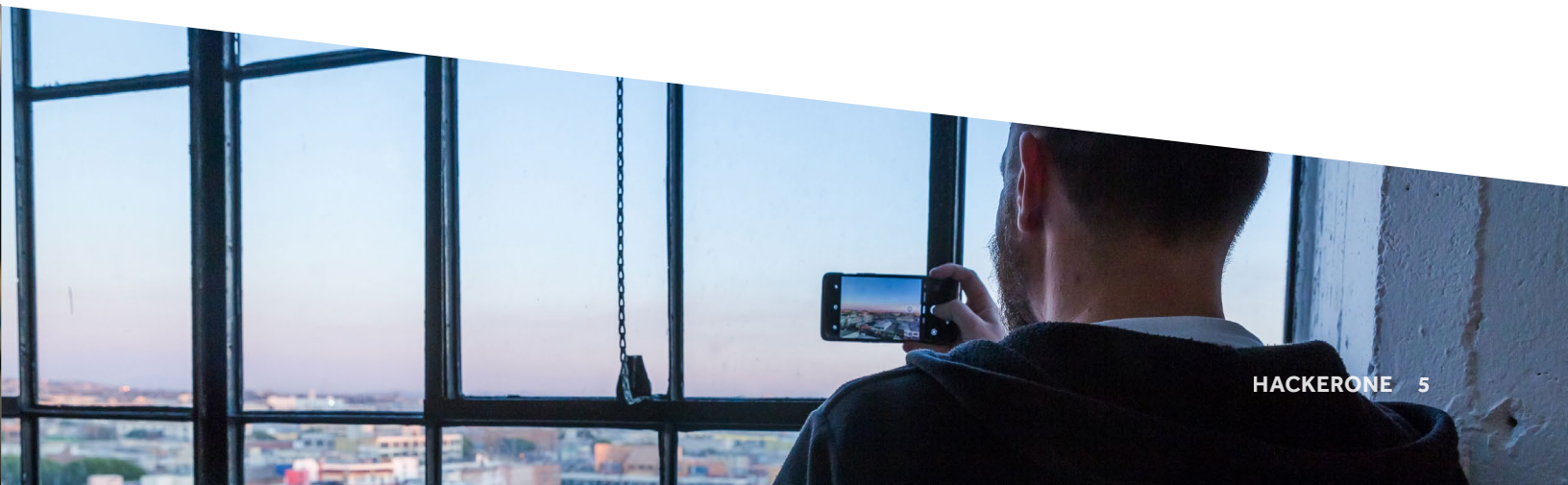
Mail.ru Group also uses incentives to attract interest at hacking conferences. The company holds hacking challenges at their booth, where winners receive a promo code for the bug bounty program. If those hackers are later awarded a bounty for a bug report, the promo code entitles them to a $100-200 bonus.

This approach has been extremely successful for the company, attracting more activity from hackers, who know that no matter what they find, they'll earn a bonus. On average, the company receives up to ten valid reports from every 150 promo codes they award, including at least one critical issue.

Vladimir stressed the importance of being flexible and creative while growing a bug bounty program and reiterated the success Mail.ru Group is seeing:

> **"As our bug bounty program has become competitive on the worldwide level, we see more engagement from all H1 researchers, including the top-ranked ones. We're very excited about what the future holds for our program!"**

.



LESSONS FROM 6 YEARS OF BUG BOUNTY

You can't run one of the world's largest bug bounty programs for six years without learning a few things. During our interview, Vladimir was generous enough to share some of the most important things he's learned by working with the HackerOne community to secure Mail.ru Group.

Lesson #1: Reward For What Your Business Needs.

Bug bounty programs are flexible. You can offer rewards for the issues that are important to your organization — for example, fraud or account hijacking — and exclude issues that aren't.

Lesson #2: Be Engaged.

The most important things you can do for your program are to respond quickly, fix reported issues, and maintain communication with your hackers.

Lesson #3: Money Isn't Everything.

You can make your program attractive without raising bounties. Hackers respect organizations that allow disclosure of findings. It allows them to publicize their successes, which encourages more hackers to take part.

Lesson #4: Start Before Release.

Providing easy access to beta functionality and offering bounties before new features are released helps to ensure that security is ingrained in the software development process, leading to a more secure product overall.

Lesson #5: Measuring Success.

Measuring success is critical for any security initiative. Vladimir Dubrovin explains: "focus on the number of critical reports first. After that, track how long it takes between the time a vulnerability is first reported to the point where it is verified, paid out and, ultimately, fixed."

WHAT'S NEXT?

After six highly successful years, the Mail.ru Group bug bounty program is still growing. Having started with just three in-scope services, the team is actively expanding the program to include other services within the Mail.ru Group. Recent additions include B2B services and several gaming websites.

Following the program's success, Vladimir believes the bug bounty program is the best way to ensure that security is upheld across the entire Mail.ru Group ecosystem.

> **"This is a massive challenge for us, and we want to invite researchers to help us implement these new properties in the most secure way," he concluded. "In the coming months, we will have plenty more opportunities for bug hunters."**

With hundreds of thousands in the HackerOne community ready to help, you don't have to go it alone.

HACKERONE HAS VETTED HACKERS FOR HUNDREDS OF ORGANIZATIONS INCLUDING:

With Over 1,800 Customer Programs,
More Companies Trust HackerOne
Than Any Other Vendor.

CONTACT US