CEQUENCE SECURITY

This Valentine's Don't Fall in Love with a Computer

There is one kind of person who isn't looking for love this Valentine's Day—

Scammers are infiltrating dating apps to build connections with legitimate users with the ultimate goal of getting them to part with their money.

In 2020, reported losses to romance scams reached a record **$304 million**.[1]

Bots allow scammers to scale their operations. Most will maximize their efforts using automation to increase their chances of success. As we saw in the movie *Her*, a single swindler often attempts to foster hundreds of romances at once, all for the possibility of more payouts.

Fake Love Starts With Fake Accounts

Fraudsters first need accounts, and lots of them, to bait other users. The two easiest ways to get them?

1 Fake Account Creation

Bad actors analyze a platform's registration business logic to find potential loopholes they can exploit to create new accounts en masse through automation.

2 Account Takeover (ATO)

A 2021 survey sponsored by Google shows that 65% of users will reuse the same password allowing scammers to leverage stolen credentials to successfully take over existing accounts on popular dating platforms and social media.

The Birds, The Bees, and The Bots

(Lots and Lots of Bots)

48% of all detected bot activity originated from the **US.**

17% of the traffic came from top US residential internet service providers.

Comcast Spectrum AT&T COX verizon CenturyLink

In 2021, Cequence Security detected (and mitigated) more than **750 million bot requests** on popular dating apps.

Cequence also protected more than **70 million** unique accounts from account takeover attempts just on a single platform.

$12,000 Average per-victim loss **PREVENTED** by Cequence.

41% of transactions were spoofing an **iPhone app.**

14% of all bot traffic came from common hosting providers.

Microsoft Azure Google Cloud aws OVHcloud DigitalOcean

Protect Your Heart and Your Wallet

While the creators of dating apps partner with companies like Cequence to detect and block bot activity on the backend. Users should also take precautions to avoid a romantic betrayal of *Ex Machina* proportions that may result in becoming a fraud victim.

Look for Red Flags	Respond Appropriately
1 You never meet in person, but things are moving fast.	Hit pause and look for authenticity of the profile and person by searching for past online activity.
2 They work overseas or make other excuses for being unavailable to meet.	Do a search or ask others online if they are being told a similar fabrication.
3 You're asked to send a gift or provide money to help them with a sudden 'emergency.'	File a fraud report[2]. **NEVER** send money, gifts, or buy tickets on behalf of someone you've never met.

Top 7 Selection Criteria to Look for in a Bot Prevention Solution

If you're a company looking for long-term protection against automated attacks, here's what you need for a perfect match.

1. **Fast Deployment and Time to Value** Able to protect your APIs and web apps in hours, not months or years.
2. **API Protection** Consistent, high efficacy protection for APIs, web and mobile apps.
3. **Ensure Broad Use Case Coverage** Make sure the solution can solve *your* specific bot challenges.
4. **Retooling Resiliency** Maintains high efficacy rates even as bots retool.
5. **Ensure User Friction** Sidestep solutions that add user-challenge-based systems like CAPTCHA and virtual waiting rooms.
6. **No Black Boxes** Access attack detection and mitigation details, create/edit policies without vendor help.
7. **Plays Well with Others** Integrates with your security ecosystem to help you improve your overall security posture.

1 https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020
2 https://reportfraud.ftc.gov

Protect Your APIs While Empowering Your Developers with Cequence Security

Organizations that rely on APIs to power their businesses trust Cequence Security to deliver the most comprehensive API Security Platform on the market. The Platform has proven to be effective in preventing unintended data leakage, online fraud, business logic attacks and exploits, which helps our F500 customers remain resilient in today's ever-changing business and threat landscape. Cequence is the only API Security Platform vendor that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving API attacks.

Schedule Your Cequence API Security Platform Demo:
cequence.ai/demo

CEQUENCE SECURITY

100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai