RSA ANTI-FRAUD COMMAND CENTER
Keeping the World Safe from Cyber Attacks for 15 Years
RSA ANTI-FRAUD COMMAND CENTER

For as long as cyber attackers have been targeting consumers, we’ve been targeting cyber attackers. Today, the RSA Anti-Fraud Command Center (AFCC) is the largest operation of its kind in the security industry—100+ analysts strong, working 24/7 from secure facilities in Israel and the United States to find and shut down cyber attacks around the world.

- First successful phishing attack against a retail bank reported in The Banker magazine
- Milestone federal regulatory guidance requires financial institutions to implement fraud prevention and risk controls
- RSA uncovers global phishing campaign to spread malware via spoofed YouTube web pages
- RSA FraudAction anti-Trojan service introduced to provide near real-time alerts of new Trojan attacks
- RSA identifies fraudulent “call center” services facilitating cashout schemes
- RSA identifies live-chat phishing attacks on users’ personal information, dubs them “chat-in-the-middle” attacks
- RSA AFCC launches the security industry’s first anti-phishing solution
- RSA® FraudAction™ Cyber Intelligence Service established by RSA AFCC to infiltrate the deep web
- 94 million credit cards exposed when weak data encryption leads to data breach of TJX Companies
- RSA exposes fraudsters launching man-in-the-middle attacks to steal OTP credentials
- Notorious carding forum DarkMarket shut down by international law enforcement
- RSA shares its extensive findings about the AS-Trovak malware hosting network
- RSA issues warnings about growing threat to corporate data posed by Trojan drop sites
RSA CyberCrime Intelligence Service established to help identify IT assets compromised by cyber attack.

RSA uncovers phishing attacks and malware trigger lists targeting hospitality and travel industry.

RSA reports public release of Carberp Trojan on dark web after developers’ failed attempt to sell it.

RSA reveals surge in dark-web cybercrime courses on card fraud, mule herding and anonymity.

RSA FraudAction Cyber Intelligence Service expanded to provide intelligence feeds to customers.

RSA reports dark-web sale of software that allows fraudsters to write stolen Track 2 data on a chip and PIN card.

RSA FraudAction Anti-Rogue App Service created in response to growing threats in the mobile channel.

RSA FraudAction 360 combines all threat vectors into a single integrated threat-fighting service.

RSA issues bombshell report on massive botnet fraud ring stealing nearly $4 billion via boleto payments.

RSA reports private financial systems developed to facilitate cashout after the takedown of Liberty Reserve.

RSA AFCC expanded to include Purdue University-based site in the US Midwest.

RSA FraudAction 360 combines all threat vectors into a single integrated threat-fighting service.

RSA released global study of 500 fraud groups on Facebook, exposing cybercrime on social media.

RSA AFCC identifies over one million phishing attacks in a single year, or one every 30 seconds.

RSA demonstrates expansion of global cybercrime to new social media platforms.

RSA AFCC identifies over one million phishing attacks in a single year, or one every 30 seconds.

RSA shows how fraudsters exploit blockchain for bulletproof hosting of online fraud forums, websites.

RSA reports dark-web sale of software that allows fraudsters to write stolen Track 2 data on a chip and PIN card.

Social media threat protection added to RSA AFCC service offerings.

RSA uncovers phishing attacks and malware trigger lists targeting hospitality and travel industry.

RSA AFCC expanded to include Purdue University-based site in the US Midwest.

RSA FraudAction Anti-Rogue App Service created in response to growing threats in the mobile channel.

RSA FraudAction 360 combines all threat vectors into a single integrated threat-fighting service.

RSA issues bombshell report on massive botnet fraud ring stealing nearly $4 billion via boleto payments.

RSA reports private financial systems developed to facilitate cashout after the takedown of Liberty Reserve.

RSA demonstrates expansion of global cybercrime to new social media platforms.

RSA AFCC identifies over one million phishing attacks in a single year, or one every 30 seconds.

RSA shows how fraudsters exploit blockchain for bulletproof hosting of online fraud forums, websites.

RSA uncovers phishing attacks and malware trigger lists targeting hospitality and travel industry.

RSA AFCC expanded to include Purdue University-based site in the US Midwest.

RSA FraudAction Anti-Rogue App Service created in response to growing threats in the mobile channel.

RSA FraudAction 360 combines all threat vectors into a single integrated threat-fighting service.

RSA issues bombshell report on massive botnet fraud ring stealing nearly $4 billion via boleto payments.

RSA reports private financial systems developed to facilitate cashout after the takedown of Liberty Reserve.

RSA demonstrates expansion of global cybercrime to new social media platforms.

RSA AFCC identifies over one million phishing attacks in a single year, or one every 30 seconds.

RSA shows how fraudsters exploit blockchain for bulletproof hosting of online fraud forums, websites.
WE FIGHT FRAUD EVERYWHERE—AND WE’VE GOT THE NUMBERS TO PROVE IT

<table>
<thead>
<tr>
<th><strong>5</strong></th>
<th><strong>18</strong></th>
<th><strong>96%</strong></th>
<th><strong>680K</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>regions served: North America, Latin America, Europe, Asia-Pacific, Japan</td>
<td>languages supported including Russian, Arabic, Spanish, French, Mandarin</td>
<td>96 percent of malicious sites blocked in less than 30 minutes</td>
<td>680,000+ malware samples analyzed monthly</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>185</strong></th>
<th><strong>1.5M</strong></th>
<th><strong>2M</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>countries where RSA AFCC has thwarted attacks</td>
<td>1,500,000+ compromised cards recovered monthly (average Jan-Sep 2018)</td>
<td>2,000,000+ attacks detected and shut down to date</td>
</tr>
</tbody>
</table>

---

**The RSA Anti-Fraud Command Center Creed**

**WE ARE HUNTERS!**
We are the eyes and ears into the cybercrime landscape, providing end-to-end visibility into its emerging threats and evolving tactics.

**WE ARE FIGHTERS!**
We take the battle to the bad guys. We detect attacks quickly and mitigate swiftly.

**WE ARE DEFENDERS!**
We protect millions of end users worldwide, and prevent billions of dollars in fraud losses. We keep the Internet safe.
PEOPLE WITH A PASSION
Meet three RSA AFCC cybersecurity specialists, united in their passion to protect RSA customers from cybercrime.

Alon Shmilovitz
Director, Head of RSA FraudAction Services

Alon Shmilovitz came to the RSA Anti-Fraud Command Center in 2007 with what seemed like a very unlikely background: Rather than hunting cybercriminals or working in any other role in the cybersecurity industry, he had been running a call center for a telecommunications company.

As it happened, Shmilovitz’s three-plus years of experience in the wireless industry was just what the RSA AFCC needed, and running an anti-fraud command center wasn’t all that different from operating a call center, what with needing to staff a 24x7x365 service, managing shifts and a relentless focus on efficiency.

When he came on board as the AFCC’s manager, Shmilovitz was charged with tripling the size of the then 40-employee operation. The unflappable Shmilovitz made the challenge look like a game of tic-tac-toe: In just two years, he had not only tripled the number of employees; he had also tripled its operational capacity while meeting all of his KPIs. For this accomplishment, Shmilovitz was promoted to senior manager and head of global AFCC operations in January 2010.

Shmilovitz’s career with RSA came full circle in 2017 when he succeeded the individual who had hired him back in 2007 and was appointed director and head of all RSA FraudAction services. That year he grew net new logos by 41 percent over 2016.

Shmilovitz says seeing results—in the form of bookings growth, revenue growth and number of attacks shut down—on a daily basis makes his job satisfying, which is not surprising for someone so focused on operations.

The hardest part of his job is when a customer, lured by the siren song of a lower price, leaves for another anti-fraud service. “We face a lot more competition today than we did 12 years ago,” says Shmilovitz. “Because we provide a service and there’s no hardware or software for a customer to install, it’s very easy for a customer to leave. That’s hard, especially knowing how much we did behind the scenes to try to retain them.”

The good news? “Many of the customers who do leave us end up coming back a year or two later,” says Shmilovitz. “They realize the service we provided really was exceptional, and the promises the other vendor made didn’t materialize.”
PEOPLE WITH A PASSION

Ktora Ben-Israel

Head of Customer Engagement & Intelligence Operations

When Ktora Ben-Israel first joined the RSA Anti-Fraud Command Center in 2006 as a contractor on a one-month project, she had no idea she’d one day be leading global customer engagement and intelligence operations teams at the largest cybersecurity company in the world.

Then 22, Ben-Israel had just returned from a trip abroad when the short-term opportunity with the RSA AFCC popped up. She put in her 30 days, and when her contract was over, she didn’t imagine that it was only the beginning of her career at RSA.

A few days after her contracting stint ended, an RSA recruiter contacted her about a full-time administrative position that was open. She ended up taking the job, and over the next five years, Ben-Israel gradually worked her way up, leading facilities management, then being named office manager. It seemed the management at RSA long saw potential in Ben-Israel that at that point she hadn’t seen in herself.

In 2011, her career took a sharp turn when she seized an opportunity to move into a customer-facing position as an engagement manager with the RSA AFCC’s FraudAction service. In this capacity, she was in charge of managing the relationship with a lengthy list of customers. Ben-Israel proved so adept in this role that she was promoted a few years later, gaining responsibility for the entire RSA FraudAction engagement management team and the global customer base it served. Then, in late 2016, she was put in charge of the intelligence team and given the mandate to forge tighter links between intelligence and engagement management. Under Ben-Israel’s careful leadership, the RSA FraudAction Cyber Intelligence Service has grown both in customer count and scope.

With several years of management experience now under her belt, Ben Israel has reached a point where she can’t imagine doing anything other than building and managing diverse global teams that cater to world-class global customers. She’s grown to love being a manager—something she never expected at the start of her career—and seeks to give her employees the growth opportunities she’s had. For example, one of her hires for the engagement management team came from an administrative position at RSA. “I recognized that this individual had extraordinary people and communication skills,” says Ben-Israel. “I thought, ‘If she can learn what we do here on the business side, she’ll be fantastic with customers.’” That hunch has proven itself: She’s been an engagement manager two years now, and she has terrific relationships with her customers.

Ben-Israel prides herself on recruiting members of her teams from all over the company and from industries outside of high-tech. “I don’t pick the obvious candidates,” she says. “I’m a strong believer in passion, motivation and fit. An individual is a whole rainbow of capabilities, and if I see potential in someone, I’ll assign them projects and responsibilities based on their strengths and interests. If you love what you do, you will be successful, and that’s what makes the RSA FraudAction team so strong.”

“I’m a strong believer in passion, motivation and fit. An individual is a whole rainbow of capabilities, and if I see potential in someone, I’ll assign them projects and responsibilities based on their strengths and interests.”
Tami Lev
Head of Business Development

Tami Lev is one of those people with the uncanny ability to identify “the next big thing” in whatever field she happens to be working in. When she worked for the California Israel Chamber of Commerce from 2007 to 2011, she helped identify the Israeli startups most likely to wow fickle Silicon Valley venture capitalists and tech companies. Two of the fledgling companies she helped select in 2009, Eyeview and SundaySky, have since matured into established leaders in the field of video marketing—a field littered with organizations that just couldn’t make it.

When Lev joined the RSA Anti-Fraud Command Center as a customer engagement manager in 2011, her ability to spot trends quickly became an asset for the company and its customers. The RSA FraudAction Anti-Rogue App service, which launched a year after Lev joined, stemmed from her work with a strategic client in banking that was struggling to fight mobile apps that used the bank’s name and brand to trick customers into forking over their personal information. The Social Media Threat Protection service that RSA unveiled in 2017 had a similar beginning, with customers struggling to address fake accounts in their companies’ names on social media sites. Lev managed the proof of concept and designed the go-to-market strategy and monetization philosophy for the social media service. Thanks in large part to Lev’s foresight and tenacity, RSA was the first in the industry to deliver these offerings.

These days, Lev and the RSA AFCC team are focused on some troubling new fraud threats. “In India, we noticed fraudsters changing the telephone numbers of certain businesses, like local banks, listed on Google Maps,” says Lev. The fraudulent telephone numbers go to call centers set up to harvest people’s personal and financial information. “This is a very, very new threat that our customers in India are experiencing.”

In Latin America, cybercriminals masquerading as global beverage companies are purporting to sell those companies’ delivery trucks on legitimate e-commerce sites. “People are paying for the trucks and not getting them, so they’re turning to the beverage companies and demanding refunds,” says Lev.

One thing Lev never predicted was how long she’d stick with RSA: Seven years is the longest she’s worked for any employer. She says the thrill of working in the cybersecurity industry with incredibly talented and passionate colleagues at RSA has kept her here—that, combined with the opportunity to do what she calls “ethical” work “fighting the bad guys” while serving clients all over the world.

“It feels like home,” Lev says of RSA. “And working with customers in every time zone on any given day makes me feel very connected.”

“Working with customers in every time zone on any given day makes me feel very connected.”
HOW TO BUILD A WORLD-CLASS ANTI-FRAUD OPERATION IN 5 STEPS

**Automate.** With thousands of cyber attacks occurring every single day, and more on the way, automation is key to keeping up. The RSA AFCC relies on a multitude of diverse, internally developed automation programs and tools that are invaluable in helping shut down cyber threats fast.

**Go global.** Worldwide coverage and support for multiple languages is essential in a time when cybercrime is everywhere. Not only that, but threats can start in one part of the world and move quickly to another, making a seamless global presence imperative to responding effectively.

**Build relationships.** You can’t fight cybercrime alone. It requires coordination and cooperation with internet hosting facilities, law-enforcement authorities and other entities around the world. Cultivating those relationships takes time, and that’s why experience count for so much.

**Go above and beyond.** Cybersecurity is a business, sure, but it’s not just any business. It’s a business where people are responsible for protecting others from potentially catastrophic cyber events—and willing to do whatever it takes to carry out that responsibility.

**Stay agile.** Threats are constantly emerging and quickly evolving. Anti-fraud operations have to be able to adapt just as fast—adopting new methodologies and techniques to root out threats, and avoiding cumbersome processes and procedures that slow things down.

TRAINING THE NEXT GENERATION OF CYBERCRIME FIGHTERS

It’s no accident that the US location of the RSA AFCC is affiliated with Purdue University, a world-renowned public research university. The location is largely staffed by computer science students working under the supervision of RSA fraud analysts and getting hands-on cybersecurity experience. That’s critical at a time when 72 percent of companies report finding it difficult to identify high-caliber cybersecurity professionals, and when ISACA projects a shortage of two million cybersecurity professionals by 2019.
ABOUT RSA

RSA® Business-Driven Security™ solutions link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com.