



# From awareness to trust

How MCF/MCC EKI Sarajevo strengthened  
security behavior across 90 locations



Financial services supported by technology and distributed operations

450+

employees

~90

locations across Bosnia and Herzegovina

30 years

supporting clients, small businesses and entrepreneurship

## Protecting trust in a regulated financial environment

MCF/MCC EKI Sarajevo is a microcredit organization with 30 years of experience in Bosnia and Herzegovina. Through nearly 90 locations and approximately 450 employees, it supports the development of small businesses, agriculture and entrepreneurship.

Operating in a regulated financial environment, the organization manages sensitive client data and depends on stable, secure operations to maintain trust and service continuity. **As digital risks progressed, cybersecurity became more than a technical requirement.** It became part of responsible business operations: protecting client information, supporting regulatory alignment and maintaining trusted relationships with clients and partners.

## The turning point: One-time awareness was no longer enough

MCF/MCC EKI Sarajevo had already been conducting security awareness training to support operational and regulatory requirements. But with a distributed workforce, increasing phishing and social engineering risks, and the need for stronger oversight, the organization recognized that periodic training could not deliver the consistency or evidence it needed.

The challenge was not simply to deliver training – it was **to build secure behavior into everyday work across all employees and locations.**

EKI Sarajevo had previously used a group-level solution with strong content quality. But because it wasn't fully adapted to the local language or operating environment, the internal team had to spend additional time on adaptation – a recurring workload. **The organization needed a model** that could scale across all locations, reduce manual effort and give the CISO function clearer visibility into progress, gaps and employee behavior.

## The strategy: Making awareness continuous and measurable

EKI Sarajevo implemented **Kaspersky Automated Security Awareness Platform (ASAP)** to create a more structured, localized and scalable awareness program.

The project was not about adding complexity to the security stack, but about a transition from a previous solution to a platform more strongly aligned with the organization's language, operating model and governance needs.

k

MCF/MCC EKI Sarajevo used Kaspersky Automated Security Awareness Platform to make security awareness more consistent, measurable and sustainable across its distributed organization, helping employees play a more active role in protecting clients, data and trusted business relationships.



By strengthening security awareness across our distributed organization, we aim to reduce risk, support our responsibility towards clients, and align our practices with European and international best practices, while contributing to trust with our business partners.

## Haris Hamidović

CISO, MCF/MCC EKI Sarajevo

# The outcomes: Stronger security, clearer oversight, less manual effort

## Highly engaged employees

with around 90% of users completing assigned training tasks within defined deadlines.

## Stronger employee response

to potential threats, with suspicious email reporting increasing from 5% to 20% – meaning four times more employees now report suspicious messages through different channels, within the first 10 minutes after the test launch.

## Reduced manual follow-up for the CISO function

through automated reminders, tracking and reporting.

## Improved visibility

into delayed or outstanding tasks, helping strengthen accountability across the awareness program.

## Reduced burden

of local content adaptation.

## Shifted security awareness

from intermittent activity to a continuous program focused on long-term behavior change.

## Improved relevance and application

with user feedback showing that the content is understandable, useful and applicable to daily operations.

## Awareness becomes action

with employees applying what they learn, reporting potential threats, seeking validation before taking action and becoming an active part of the organization's security posture.

## Internal resources freed-up

to focus on analysis, monitoring and continuous improvement instead of manual administration.



**Kaspersky  
Automated Security  
Awareness Platform**

## Kaspersky Automated Security Awareness Platform **enabled:**

- Role-based and adaptive learning paths
- Continuous training integrated into daily work
- Phishing simulations and behavioral reinforcement
- Centralized reporting and measurable progress tracking
- Automated reminders and visibility into incomplete tasks
- Consistent delivery of awareness content across all employees and locations
- Reporting to support audit requirements and CISO oversight

## The business impact: Protecting clients, supporting compliance and building sustainable awareness

In regulated environments, demonstrable evidence of employee awareness is important for internal audit expectations, regulatory alignment and security oversight. Kaspersky ASAP **gives the CISO function clearer visibility into participation, progress and outstanding tasks, while helping the security team implement structured awareness activities** aligned with ISO 27001 compliance requirements.

Improved awareness and increased reporting of suspicious emails contribute to reducing the risk of successful phishing incidents, while Kaspersky ASAP also supports audit and compliance requirements, helping EKI Sarajevo demonstrate a more structured and sustainable approach to human risk.

By integrating awareness into its broader governance and risk management framework, EKI Sarajevo has made security awareness an ongoing process rather than a one-time activity. This supports **protection of sensitive client data, human risk management, regulatory alignment and resilience against common cyberthreats.**

Looking ahead, the organization expects continued platform development in areas such as content updates, localization quality and user experience. Stable vendor support and predictable pricing also remain important for long-term planning.



# Kaspersky Automated Security Awareness Platform

Try now

[www.kaspersky.com](https://www.kaspersky.com)

© 2026 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.

#kaspersky  
#truetobusiness