TRAINING BANK EMPLOYEES TO RECOGNIZE PHISHING ATTEMPTS



RAVNAQ-BANK

HWG Sababa

Case study

About Ravnaq Bank

Provides bank services to businesses and consumers since 2001

Operates throughout Uzbekistan

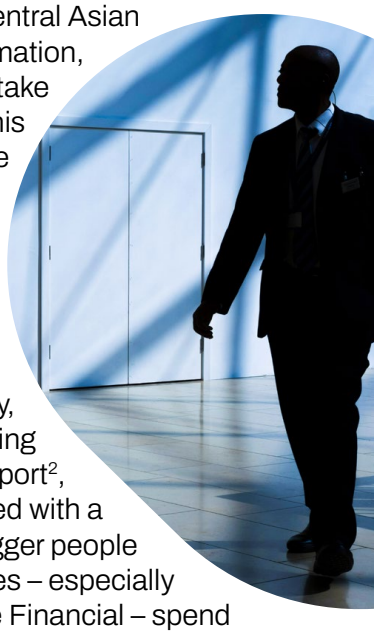
Gains its HQ in Tashkent and employs almost 150 specialists

First bank in Uzbekistan to launch contactless smartphone payments with Mastercard

"We see the importance of complex measures to address the security risks. These include ongoing security monitoring, incident response plan, and user training to minimise human mistakes and increase the overall security resilience of the bank"

Abdukakhor Tulyaganov, Head of Bank Security.

Cybersecurity in Uzbekistan



Remaining among the major cyberthreats in Europe[1], phishing is also a big deal for businesses in the Central Asian countries. On the way of the digital transformation, cybercriminals exploit every opportunity to take advantage of the corporate network. This includes exploiting the human factor, like making common users conduct unsafe actions to share credentials and other sensitive data, as well as technically open access to the bad guys through the corporate perimeter security breach.

To make people behave insecurely, cybercriminals manipulate emotions. According to the recent HWG Sababa Awareness Report[2], greed, curiosity and a wish to help combined with a sense of urgency or authority of a sender trigger people more than anything else. Therefore, companies – especially those working in sensitive verticals like Financial – spend their effort to train their employees and empower them with the necessary knowledge and skills to recognize, filter out, and report any suspicious communications.

This attitude allows using the human factor for the benefit of the organisation, turning their employees into the company's additional layer of protection both for the business and their clients. This is what Ravnaq Bank timely recognized too.

Challenges and goals

Operating for over 20 years, Ravnaq Bank is modern and innovative. It has its headquarter in Tashkent and does not run any other branch offices, conducting all the financial operations virtually. It is one of the first banks in Uzbekistan to have launched a smartphone app for online bank operations and e-commerce, speeding up and simplifying business activities for several clients all over the country, including large food producers and healthcare organisations.

Innovation comes alongside security. 2 years ago, when Ravnaq Bank released its online bank app, it acted strategically and shared the cybersecurity responsibilities with the other security functions of the bank. Following the digital transformation trends, it recognized the insecure behaviour among its employees and the importance of growing security awareness among them.

HWG Sababa

RAVNAQ-BANK

[1] Rapporto Clusit sulla Sicurezza Informatica 2022
[2] HWG Sababa Awareness Report 2021

"We noticed a complex of user issues during one of the internal assessment activities. Those included the usage of primitive passwords to log into computers and smartphones, overlooking the personal cybersecurity basics like locking the PCs when leaving the work desk, as well as data processing mistakes",

commented Abdukakhor Tulyaganov, Head of Bank Security

"We have a comprehensive security policy standard, which we update on a monthly basis and approve with the Cybersecurity Center of Uzbekistan. In addition to controlling the situation with security policies, we decided to focus on the training for our specialists too".

However, at Ravnaq Bank they quickly realised that conducting cybersecurity training requires specific knowledge, skills and time. Therefore, having only 2 dedicated specialists to address all the cybersecurity areas, they decided to unite efforts with the IT department and the Training team. Together they convinced the Board of Directors to support the awareness investment as a strategic step, even if the ROI could have taken time and be invisible in preventing cybersecurity incidents caused by human mistakes.

"We didn't lose much time when considering an offline course, as our experience showed that it often lacks regular practical training. We needed a solution that would not distract employees from work, would be easy to use, especially in the morning hours, and which would refresh the user's knowledge every 3 months. It was also important for us to be able to train our specialists in Uzbek and Russian"

explained Abdukakhor Tulyaganov,

"This is why we were glad to be introduced to HWG Sababa".

One of the main reasons that made the bank's choice fall on HWG Sababa Awareness platform is the combination of its generic and specific training modules with phishing attack simulations, localised into Uzbek and Russian. Before proceeding with the project, Ravnaq Bank decided to test the online training platform on a small group of users. The Proof of Concept (POC) took 1 week.

"We conducted a phishing attack simulation to test the overall readiness of our colleagues to react to a cyber-attack. It was a nice surprise to discover that our employees behaved better than expected. Only few of them made some insecure actions with the test email, while the others started immediately calling the technical support to report suspicious messages",

said Abdukakhor Tulyaganov,

"The simulation effect was positive, and we decided to proceed with the project".

The Ravnaq training plan includes 2 main stages:

Upskill the entire IT and Security teams first, so that they would be ready to supervise the awareness training towards the others

Train the retail team, which works with the physical clients and their data, mobile banking app, and bank cards

Results

The experience of Bank demonstrates the importance of a strategic approach to innovative technologies and their cyber safe application.

“Fraud and phishing attack attempts are growing exponentially, especially on weekends and late at night. Therefore, we see the importance of complex measures to address the security risks”,

concluded Abdukakhor Tulyaganov,

“These include ongoing security monitoring, incident response plan, and user training to minimise human mistakes and increase the overall security resilience of the bank”.

HWG Sababa

RAVNAQ-BANK

Follow us on:

www.hwgsababa.com