

# Cyber Security



# Fraud protection



Provide regular fraud training to employees with real-life examples

## Email

Train employees on email security and necessary verification of sender addresses, files and links from untrusted sources.

## Social engineering

Train your employees to identify signs of social engineering, e.g. manipulating phone calls or requests of personal information.

## Identity of a partner in conversation

Verify the identity of the partner in phone conversation, especially for non-standard requests (The Police Department, the National Bank, etc.), and do not share personal data.

# Cyber Security



## Important actions

- Differentiate access to information within the organization
- Use and regularly update **only licensed software** and antivirus databases on all devices on which you use Onlinebank. To improve security, schedule AutoUpdate to update every 10 minutes
- Do not disclose your personal information on social media
- Use **two-factor authentication** to log in to important business systems.
- Do not give anyone access to your computer or workplace and **lock your computer** before leaving



Use personal accounts and strong passwords when working in corporate systems

# Physical Security



Install CCTV cameras in legally authorized locations



Install an access control and management system (ACMS)



Keep a record of all visitors to your office



Store confidential documents in a lockable shelf/safe deposit box



Destroy printed confidential documents using paper shredder



To ensure safety of your office, you can also place it in a facility with security guards

# Virus in emails

## Negative Trends in Cyber Security

Fraudsters may send emails on behalf of a counterparty, bank or government agency with information about company operations or violations

The email attachment may contain a virus that is activated when the email is opened. It may be invisible to anti-viruses and it may collect and transmit sensitive information such as payment details, account numbers, passwords, etc. to scammers/fraudsters.

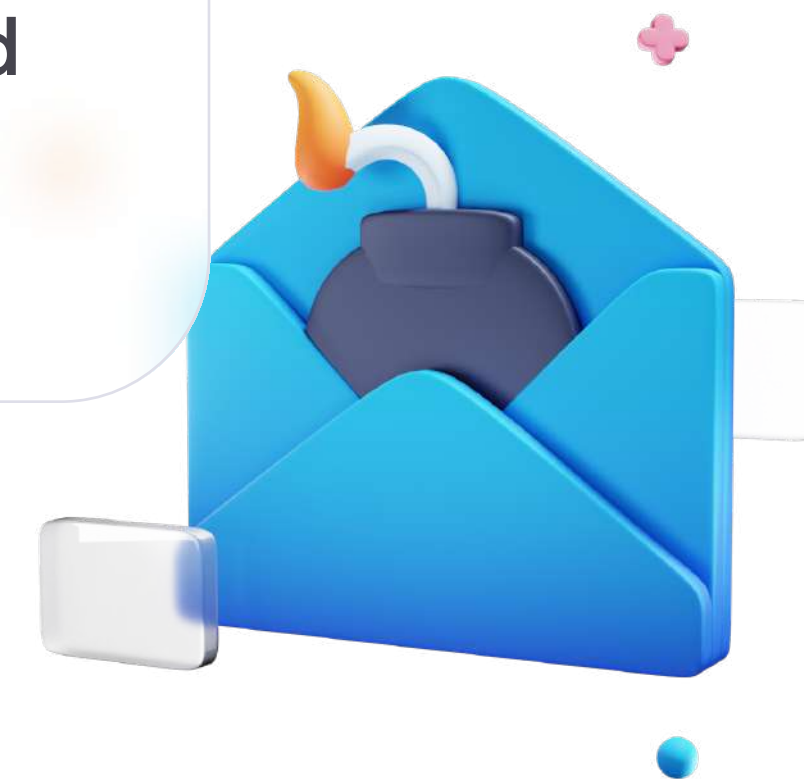
The virus can modify payment amounts and recipient details or give the fraudsters remote access to your device to steal information and manage online banking at the moment of sending payment, etc.



# An unreliable outsourcing company

Negative Trends in Cyber Security

You hired a company to administer and maintain computers and systems that turned out to be unreliable. While performing its duties, its representative plugged in an infected USB flash drive, which transmitted a virus to your compute



# Third Party Access

## Negative Trends in Cyber Security

Employees of your company treat information security light-heartedly and leave sticky notes with password on their desks.

Besides, a cleaning company has access to your office, and its staff can get the password to an employee's account during cleaning.

This data can be sold to cybercriminals on the internet who can use it to cyberattack your network.

Negligence related to electronic digital signature (EDS) when an executive provides it to an employee enabling him/her to sign documents on behalf of the executive.

This can lead to illegal acts such as making bogus transactions and forging of invoices signed with the executive's EDS.

If criminals gain access to the EDS, you may lose all funds on the company's accounts and the company itself as they can re-register documents using your EDS.

# Security Measures for Working with **ONLINEBANK**

## Input devices

- Do not give them to third parties
- Do not leave them connected to a computer in your absence

## Personal or corporate email address

- Check the sender's address and be careful about urgent request
- Do not click on suspicious links or and do not open doubtful files

## Software and Antivirus

- Do not install remote management software (TeamViewer, AmmyyAdmin, AnyDesk, RustDesketc.)
- Check if the website has an encrypted connection and an authentic certificate  `onlinebank.kz`  `halyk.onlinebank.kz`
- Use and regularly update only licensed software and antivirus databases on all devices on which you use Onlinebank.  
To improve security, schedule AutoUpdate to update every 10 minutes
- Use Windows Defender SmartScreen filter in Microsoft Edge browser



# Security Recommendations for **ONLINEBANK**

## Transaction control

- Install Onlinebank and activate notifications on account movements
- Set up several signature levels (primary signature authority - Director and secondary signature authority - Chief Accountant).
- Additional user can be added in the More section of Onlinebank app

## Be attentive to your partners

- When you receive new details of your partners, we recommend calling them and confirming the change of details



**Feel suspicious?  
Call us!**

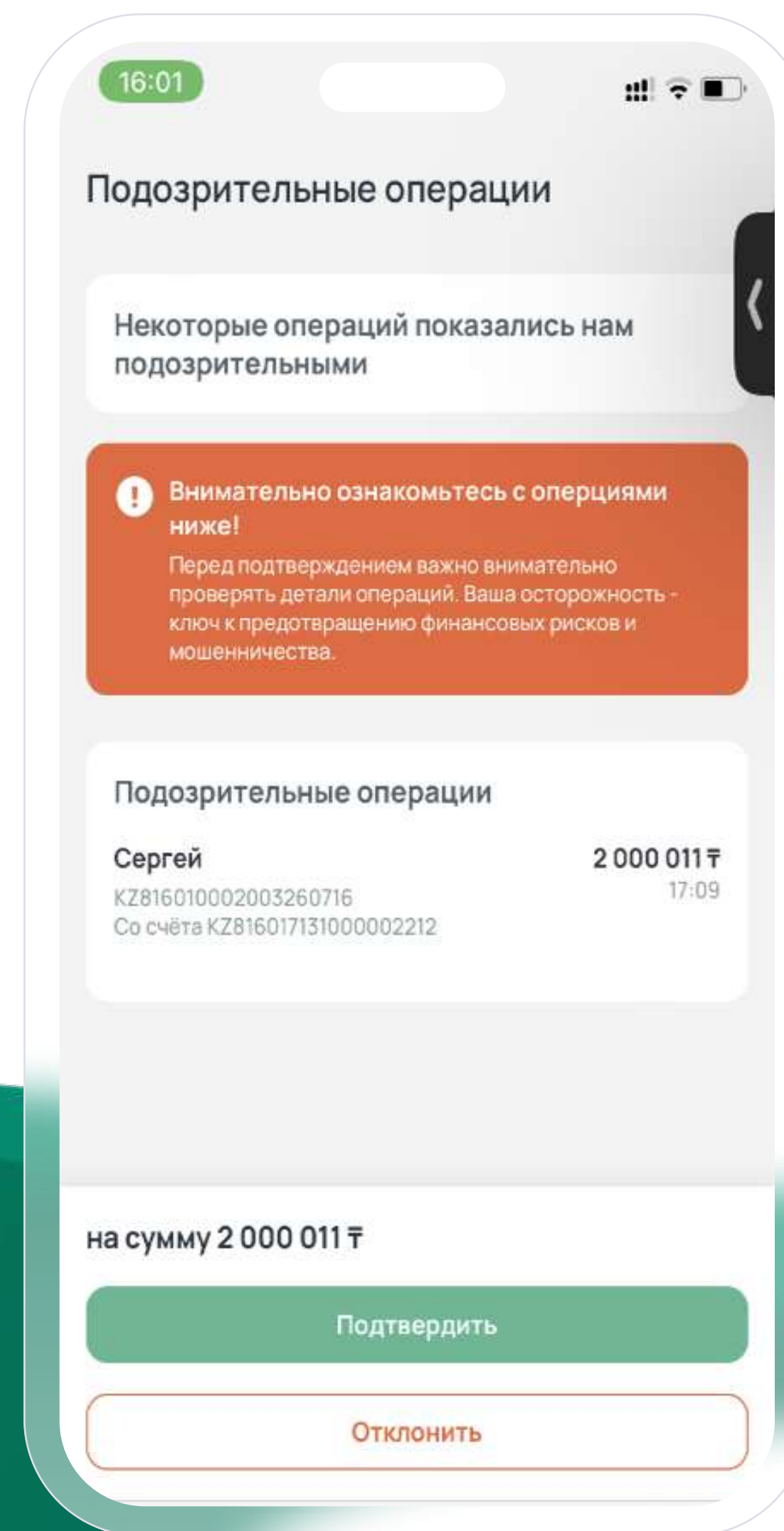
In case of unconfirmed transactions, please contact the Bank's Contact Centre.

### Contact Centre for legal entities and individual entrepreneurs

- 9595 (calls are free of charge from mobile phones)
- 8(727)259-07-77 (Almaty)
- 8 8000 8000 59 (free of charge within Kazakhstan)

# A suspiciousness Check

- Halyk checks and analyzes all transactions for fraud using fraud analytics
- If transactions are suspicious, we may send an SMS/Push notification or call you to confirm payments for additional verification
- If you have not received SMS/Push notification, set up a trusted number at the Bank's outlet
- Waiting time for confirmation is 30 minutes
- The Bank operator will call you later on to confirm the transaction



# Fake apps in AppStore and Google Play

- When downloading Onlinebank app, check that its owner is **Halyk Bank JSC**. If the owner is different, they are scammers who want to cheat and steal money
- Do not download apps from SMS links or from unknown senders in messengers
- Look at user reviews and ratings of the app and whether it is possible to leave a comment
- Legitimate apps always describe their functions in the **Data Security** section. Check if this section is present

## ✓ Official

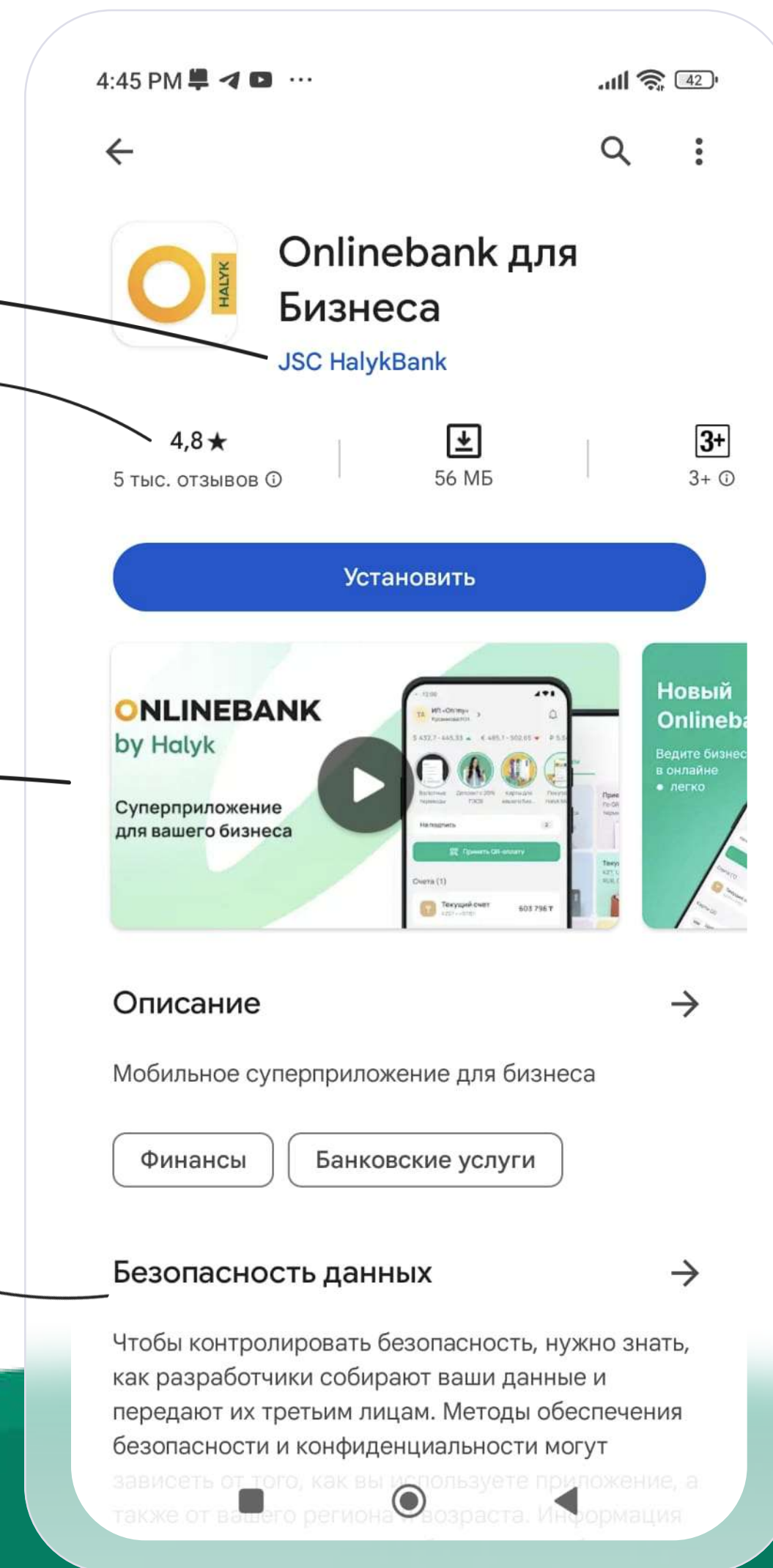
## ! Fake

Корректное  
Name of the owner

Reviews and comments  
are authorized

A video footage and  
information on the app  
is available

Section on the security is available



Suspicious owner

Reviews and  
comments are  
banned

There are no further  
details on the app

Section on the  
security is absent

