Платформа цифровых активов

Общество с ограниченной ответственностью
«Токены – Цифровые Инвестиции» (ООО «Токены»)

УТВЕРЖДЕНЫ
приказом от 21.08.2026 № 22597-П

РЕКОМЕНДАЦИИ

по обеспечению информационной безопасности при совершении финансовых операций

Клиентская памятка во исполнение пункта 1.13 Положения Банка России № 757-П

Редакция для доведения до клиентов

(версии 1.0)

ИСТОРИЯ ИЗМЕНЕНИЙ ДОКУМЕНТА

Дата утверждения	Номер приказа	Номер версии	Изменения
21.08.2026	22597-П	1.0	Утверждение документа

Оглавление

1. Назначение

Настоящие рекомендации разработаны в целях защиты клиентов от мошеннических действий, предотвращения несанкционированного доступа к защищаемой информации и снижения риска совершения незаконных финансовых операций.

2. Возможные риски несанкционированного доступа

При использовании дистанционных сервисов существует риск получения злоумышленниками доступа к вашим персональным данным и денежным средствам.

- заражение устройства вредоносным программным обеспечением;
- получение доступа к логину, паролю, PIN-коду и одноразовым кодам подтверждения;
- фишинговые сайты и поддельные мобильные приложения;
- телефонное мошенничество и социальная инженерия;
- использование похищенного или потерянного мобильного устройства;
- подключение к небезопасным сетям Wi-Fi;
- использование устаревшего программного обеспечения;
- установка программ из непроверенных источников;
- получение доступа к данным через программы удаленного управления устройством.

3. Защита от вредоносного программного обеспечения

Для снижения риска заражения устройства рекомендуется:

- использовать лицензионную операционную систему;
- своевременно устанавливать обновления операционной системы;
- регулярно обновлять браузер и иные используемые приложения;
- устанавливать приложения только из официальных магазинов приложений;
- не отключать встроенные механизмы защиты устройства;
- использовать антивирусное программное обеспечение и поддерживать его базы в актуальном состоянии;
- регулярно выполнять проверку устройства на наличие вредоносного программного обеспечения;
- не открывать подозрительные вложения электронной почты и сообщения от неизвестных отправителей;
- не переходить по неизвестным или подозрительным ссылкам;
- не подключать неизвестные USB-носители.

4. Защита учетных данных

Для защиты доступа к финансовым сервисам рекомендуется:

- использовать сложные уникальные пароли;
- незамедлительно менять пароль при наличии подозрений на его компрометацию;
- использовать двухфакторную аутентификацию при наличии такой возможности;
- не сохранять пароли в открытом виде;
- использовать надежный менеджер паролей.

Никому не сообщайте:

- пароль;
- PIN-код;
- CVV/CVC-код карты;
- коды из SMS;
- push-коды подтверждения;
- одноразовые пароли.

5. Безопасная работа с мобильным устройством

Рекомендуется:

- установить пароль, PIN-код или биометрическую защиту устройства;
- использовать автоматическую блокировку экрана;
- включить функцию поиска устройства;
- включить возможность удаленного удаления данных;
- использовать шифрование памяти устройства;
- не предоставлять устройство посторонним лицам;
- не использовать устройство с root-доступом или jailbreak;
- отключить установку приложений из неизвестных источников.

6. Контроль конфигурации устройства

Перед использованием дистанционных финансовых сервисов рекомендуется убедиться, что:

- операционная система обновлена;
- антивирусное программное обеспечение и его базы обновлены;
- браузер обновлен;
- отсутствуют подозрительные приложения;
- отключена установка программ из неизвестных источников;
- не отключены встроенные средства защиты;

- используются только официальные приложения организации.

Регулярно проверяйте список установленных приложений, предоставленные им разрешения и удаляйте неизвестные или неиспользуемые программы.

7. Безопасное использование сети Интернет

Рекомендуется:

- использовать защищенные сети связи;
- избегать подключения к публичным сетям Wi-Fi при совершении финансовых операций;
- проверять адрес сайта перед вводом данных;
- использовать только официальный сайт и официальное приложение организации;
- обращать внимание на наличие защищенного соединения (HTTPS), но не считать его единственным признаком подлинности сайта.

8. Признаки мошенничества

Следует проявлять особую осторожность, если:

- вам звонят от имени организации и требуют срочно перевести денежные средства;
- просят сообщить пароль или код из SMS;
- предлагают установить неизвестную программу;
- убеждают предоставить удаленный доступ к устройству;
- присылают ссылки на неизвестные сайты;
- требуют выполнить действия под предлогом защиты денежных средств.

Сотрудники организации не должны запрашивать пароль, PIN-код, одноразовые коды, CVV/CVC-код карты или коды подтверждения операций.

9. Действия при утрате (потере, хищении) устройства

При потере мобильного телефона, планшета или компьютера необходимо незамедлительно:

- Заблокировать доступ к личному кабинету.
- Сообщить об утрате устройства в организацию по официальным каналам связи.
- Заблокировать SIM-карту у оператора связи.
- При наличии возможности выполнить удаленную блокировку и удаление данных.
- Сменить пароль доступа.
- Проверить историю финансовых операций.

- При обнаружении подозрительных операций немедленно сообщить в организацию.

10. Признаки возможного заражения устройства

Следует немедленно прекратить использование устройства для совершения финансовых операций, если наблюдаются:

- самопроизвольная установка приложений;
- необычно быстрый расход аккумулятора;
- неизвестные SMS или уведомления;
- всплывающая реклама;
- неожиданные запросы дополнительных разрешений;
- самопроизвольный запуск программ;
- существенное замедление работы устройства;
- невозможность установить обновления.

При наличии указанных признаков рекомендуется:

- отключить устройство от сети Интернет;
- выполнить проверку актуальным антивирусным программным обеспечением;
- обратиться к квалифицированным специалистам;
- не совершать финансовые операции до устранения проблемы.

11. Рекомендации при совершении финансовых операций

Перед подтверждением операции рекомендуется:

- проверить реквизиты получателя;
- убедиться в правильности суммы;
- проверить назначение платежа;
- убедиться, что операция инициирована лично вами.

После совершения операции рекомендуется:

- контролировать историю операций;
- подключить уведомления о финансовых операциях;
- регулярно проверять остаток денежных средств.

12. Если вы подозреваете мошенничество

Немедленно:

- прекратите выполнение операции;

- смените пароль;
- заблокируйте доступ к сервису;
- сообщите в организацию по официальным каналам связи;
- обратитесь в правоохранительные органы при необходимости.

Соответствие требованиям пункта 1.13 Положения № 757-П

Матрица показывает, в каких разделах настоящих рекомендаций раскрыты элементы требования.

Требование	Раздел документа
Рекомендации по защите от вредоносного кода	Разделы 3, 6, 10
Информация о рисках несанкционированного доступа	Разделы 2, 8
Меры по предотвращению несанкционированного доступа	Разделы 3–8, 11
Действия при утрате устройства	Раздел 9
Контроль конфигурации устройства	Раздел 6
Своевременное обнаружение вредоносного кода	Раздел 3 и 10

Настоящий документ охватывает содержание рекомендаций и информации, перечисленных в пункте 1.13 Положения Банка России № 757-П, и может использоваться в качестве официальной памятки для клиентов.

Организации рекомендуется дополнительно утвердить внутренний порядок информирования клиентов, определить каналы и периодичность доведения рекомендаций, обеспечить их актуализацию и сохранять подтверждения размещения или направления клиентам.