БАНК ОРЕНБУРГ

Акционерное общество коммерческий банк «ОРЕНБУРГ»

РЕКОМЕНДАЦИИ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемый клиент!

В случае, если вы столкнулись с признаками компрометации при работе в Интернет-банке или мобильном приложении (несанкционированные операции, блокировка или шифрование файлов, необычное поведение программ), просим вас действовать максимально оперативно и аккуратно. От ваших первых шагов напрямую зависит возможность расследования, сохранность данных и минимизация финансовых потерь.

Ключевое правило — не пытаться устранить угрозу самостоятельно (удалять файлы, лечить антивирусом). Ваша задача - зафиксировать следы инцидента в текущем состоянии.

Вне зависимости от типа устройства (ПК или мобильное устройство) **НЕ РЕКОМЕНДУЕТСЯ**:
– перезагружать или выключать устройство (за исключением мобильных устройств с eSIM);
– запускать антивирусное сканирование для лечения или удаления угроз;
– производить очистку временных файлов, кэша или корзины;
– самостоятельно удалять подозрительные файлы или программы;
– совершать любые действия, изменяющие текущее состояние системы (установка/удаление ПО).

Если инцидент произошёл на стационарном компьютере, ноутбуке или моноблоке:

1. Извлечение ключевых и съёмных носителей:
Не закрывая активных окон, в первую очередь:
– физически извлеките все ключевые носители (токены, смарт-карты, USB-ключи ЭЦП);
– извлеките съемные носители информации (флеш-накопители, внешние жесткие диски, карты памяти), не производя на них запись. Оставьте носители в том состоянии, в котором они находились на момент инцидента.

2. Изоляция устройства от сети:
Для предотвращения распространения вредоносной активности и несанкционированного удалённого доступа:
– физически отключите сетевой кабель (Ethernet) от компьютера;
– при использовании Wi-Fi отключите беспроводной адаптер (аппаратным переключателем или через системный переключатель в меню «Сеть» на ПК). **Не завершайте системные процессы для отключения сети**.
– Устройство должно оставаться включенным, а система – загруженной.

3. Сохранение образца вредоносного ПО:
– скопируйте подозрительный файл(ы) на внешний носитель, не запуская и не открывая его.
– упакуйте файл(ы) в ZIP-архив и установить на него пароль. **Сообщите пароль сотруднику Банка только по защищенному каналу**;
– зафиксируйте путь к файлу, его размер и дату изменения (допускаются скриншоты экрана).

Если инцидент произошёл на мобильном устройстве (смартфон/планшет):

– немедленно включите **«Авиарежим»** - это разорвёт все сетевые соединения (сотовая связь, Wi-Fi, Bluetooth, NFC);

– не закрывайте активные приложения и не сворачивайте их принудительно – это может стереть следы инцидента из оперативной памяти устройства.
– извлеките физическую SIM-карту;
– если в устройстве используется только электронная SIM-карта (eSIM), извлечь которую невозможно, допускается полное выключение устройства для разрыва сетевой активности. При этом следует учитывать, что выключение приведет к потере содержимого оперативной памяти, но позволит избежать дальнейшего распространения атаки.

Категорически запрещено на мобильном устройстве:
- **выполнять сброс** до заводских настроек (Hard Reset);
- использовать встроенные функции **«очистки»** и **«оптимизации»** системы;
- **удалять** приложения и данные вручную.

После выполнения рекомендаций:

1. **Уведомите Банк** об инциденте по установленным каналам связи (телефон клиентской поддержки, официальный адрес электронной почты);
2. **Обеспечьте сохранность** доказательств (образов памяти, дисков, файлов вредоносного ПО) в неизменном виде до момента их передачи в Банк для проведения расследования;
3. **Задокументируйте** время обнаружения инцидента, предпринятые действия и контактные данные лиц, участвовавших в фиксации доказательств (при наличии).

Соблюдение настоящих рекомендаций критически важно для установления причин инцидента и минимизации ущерба. Банк окажет необходимое содействие в проведении расследования.