

## **Внимание клиентов Банка!**

В последнее время участились атаки мошенников на клиентов Банков, целью которых является хищение денежных средств клиентов через Систему Дистанционного банковского обслуживания для физических лиц (далее Система ДБО).

Для организации атаки злоумышленники используют уязвимости в операционных системах, в средствах защиты и человеческой невнимательности.

Одним из основных источников заражения является так называемая фишинговая рассылка электронных писем. Злоумышленники часто рассылают электронные письма от сторонних легитимных организаций или от имени компаний партнеров. Такие электронные письма как правило содержат вложения (документы или архив, зараженный вредоносной программой) или просьбу перейти на Интернет сайт, содержащий вредоносный контент. При открытии вложения или при переходе по ссылке происходит заражение **компьютера** или **смартфона, планшета** (далее **Устройство**) вирусом, при помощи которого злоумышленник получает удаленный контроль над **Устройством**, а также получает доступ к конфиденциальной информации.

Так же злоумышленники используют фейковые сайты известных фирм, банков и Государственных органов власти. Перейдя на фейковый сайт происходит заражение вирусом, при помощи которого злоумышленник получает контроль над **Устройством** клиента, а также получает доступ к конфиденциальной информации.

Попадая на **Устройство** клиента, злоумышленники анализируют используемые ресурсы, ищет Системы ДБО и начинает изучать работу клиента в Системе: время работы клиента в Системе ДБО, выключается ли компьютер после окончания рабочего дня, изымаются ли носители с секретными ключами или нет. Такой анализ может занимать от нескольких дней до нескольких месяцев и затем перехватывает пароли от Системы ДБО.

Далее злоумышленники ждут подходящего момента для формирования и отправки в Банк мошеннических переводов. Мошеннические переводы могут быть сформированы вместе с платежами клиента или в момент минимальной активности клиента (к примеру, в ночное время или в час-пик, пока Вы едете общественном транспорте и у Вас нет возможности пользоваться **Устройством**).

После формирования мошеннического перевода и отправки его в Банк, злоумышленники меняют пароль доступа к Системе ДБО, блокируют доступ

к **Устройству** или разрушают логическую структуру памяти **Устройства** (стирают (форматируют) память **Устройства**), тем самым блокируя доступ к Системе ДБО и лишая клиента возможности проверить платежи и остаток на счете.

**В связи вышеизложенным, АКБ «ФОРА-БАНК» обращает Ваше внимание на соблюдение требований безопасности при пользовании Интернет-банкинга «ФОРА-ОНЛАЙН».**

1. При получении электронных сообщений необходимо быть внимательным никогда не открывать подозрительные файлы или переходить по ссылкам на подозрительные Интернет ресурсы.
2. Используете на компьютерах, смартфонах, планшетах антивирусное ПО, поддерживайте его антивирусные базы в актуальном состоянии. Проводите периодическое полное антивирусное сканирование Устройства (рекомендовано раз в неделю).
3. Никогда и никому не сообщайте пароль от Интернет-банка.
4. Используйте сложный пароль для входа. Не используйте Вашу дату рождения, фамилию, имя и другие известные факты.

Пароль должен содержать:

- Минимум – 8 символов;
  - Заглавные и строчные латинские буквы;
  - Цифры;
  - Спецсимволы ( ` @#\$&\* и т.п.).
5. Не храните на своем Устройстве средства доступа к системам дистанционного банковского обслуживания (*логины и пароли*), номера карт, паспортные данные и прочую конфиденциальную информацию, чтобы она не стала доступна третьим лицам в случае утраты устройства.
  6. Не используйте общедоступные сети Wi-Fi для подключения к системам дистанционного банковского обслуживания.
  7. При поступлении звонков, СМС-сообщений, а так же сообщений в социальных сетях и мессенджерах с просьбой предоставить информацию касающуюся финансовых операций (*подозрительный платеж, Ваша карта заблокирована, проблемы с проведением операции и т.п.*)
    - Не перезванивать на указанные в сообщениях номера;
    - Не сообщать звонящим разовые коды подтверждения операции, данные банковских карт: *номер карты, срок действия, CVC / CVV (с*

*обратной стороны карты), а также персональные данные: серия и номер паспорта, адрес регистрации.*

8. При проведении операций проверяйте суммы платежей и реквизиты операции в СМС-сообщении, содержащем разовый пароль. Информация должна совпадать с Вашей операцией в «Фора-Онлайн», которую Вы хотите подтвердить. Если полученная информация отличается, не вводите разовый пароль и незамедлительно сообщите об этом в Банк в Службу технической поддержки – 8 (800) 100-98-89.
9. Используйте для звонков в Банк номер телефона, указанный на Вашей карте. Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть не доступны или по ним ответит оператор, который будет пытаться Вас обмануть.

**В целях снижения риска несанкционированного доступа к Мобильному Банку и поддержания его в работоспособном состоянии:**

10. Устанавливайте Мобильный Банк из официальных источников, рекомендуемых Банком (Google Play или App Store).
11. На мобильном **Устройстве** используйте операционную систему, соответствующую минимальным требованиям, размещенную на сайте Банка.
12. Своевременно обновляйте операционную систему мобильного устройства.
13. Своевременно обновляйте Мобильный Банк.
14. При наличии технической или функциональной возможности мобильного устройства, используйте средства защиты от воздействия вредоносного программного кода (антивирус). Своевременно обновляйте антивирусное программное обеспечение и антивирусные базы. Проводите периодическое полное антивирусное сканирование мобильного устройства (рекомендовано раз в неделю).
15. При наличии технической или функциональной возможности мобильного устройства, установите дополнительный режим защиты доступа к мобильному устройству (вход по код-пароллю, отпечатку пальца и т.п.).
16. При проведении операций проверяйте суммы платежей и реквизиты операции в СМС-сообщении, содержащем разовый пароль. Информация должна совпадать с Вашей операцией.

В случае выявления аномалий на Вашем **Устройстве** или в **Системе ДБО** (не можете войти в Систему ДБО, произвольное мерцание экрана, движение



мыши, произвольное открытие и закрытие окон, программ и т.п.), обнаружили совершение или попытку кражи денежных средств, незамедлительно отключите **Устройство** и обратитесь в АКБ «ФОРА-БАНК» (АО) по телефонному номеру **8 (800) 100-98-89**.

При утрате (потере, хищении) Вашего Устройства, для предотвращения несанкционированного списания Ваших денежных средств незамедлительно обратитесь в АКБ «ФОРА-БАНК» (АО) по телефонному номеру **8 (800) 100-98-89**.

**Служба информационной безопасности  
АКБ «ФОРА-БАНК» (АО).**