Управляющая компания ПЕРВАЯ

Телефон +7 (495) 258 05 34
Факс +7 (495) 258 05 36
www.first-am.ru

Правила информационной безопасности

Памятка для клиентов АО УК «Первая»

Ваша безопасность — наш приоритет

Мы заботимся о сохранности ваших персональных данных и средств на ваших инвестиционных счетах, используем современные средства защиты и блокируем новые угрозы. Но не менее важна ваша собственная осторожность при совершении финансовых операций.

Ваша бдительность — лучшая защита

Ваши счета недоступны для злоумышленников, если вы соблюдаете правила информационной безопасности. Не пренебрегайте ими при использовании устройств, с которых заходите в дистанционные сервисы банка и управляющей компании.

Общие правила безопасности

Храните в тайне конфиденциальные данные

- Никому не сообщайте пароли, СМС-коды, кодовые слова, ключи электронной подписи и шифрования, пин- и CVV-коды от банковских карт.
- Будьте бдительны, если вам звонят или пишут якобы от имени банка или компании с просьбой поделиться паролями. Сотрудники АО УК «Первая» и банка никогда не просят сообщить пароли и другие конфиденциальные данные. Кодовое слово у вас попросят только если вы сами звоните в контактный центр.
- Старайтесь без большой необходимости не сообщать кому-либо номера ваших счетов, паспортные данные, номера банковских карт. Для интернет-покупок заведите отдельную карту.

Будьте осторожны при получении электронной почты, СМС и звонков от неизвестных

- Не открывайте подозрительные письма и вложения к ним, полученные от неизвестных отправителей: мошенники могут заразить ваш компьютер или телефон вирусом и украсть ваши данные.
- Внимательно проверяйте, от кого пришло СМС-сообщение или электронное письмо. Отправителем может оказаться злоумышленник, который маскируется под представителя компании или банка.
- Не переходите по подозрительным ссылкам в электронных письмах и СМС. Если вы перешли по ссылке и вас просят ввести пароли, будьте бдительны: мошенники таким способом пытаются получить доступы к счетам. Проверяйте ссылки на веб-страницы: адреса поддельных сайтов могут немного отличаться от официальных сайтов компании и банка.

  Официальные сайты:
  АО УК «Первая»: https://www.first-am.ru
  ПАО Сбербанк: https://www.sberbank.ru

- Будьте особенно осторожны, если люди, представившиеся сотрудниками банка или компании, требуют от вас быстрых действий (уточнить реквизиты карты, срочно позвонить по указанному номеру или перейти по ссылке), пытаются напугать («Ваш счёт заблокирован») или сообщают о каком-то выигрыше. Это распространенные приёмы мошенников.

При любом подозрении на мошенничество обратитесь в компанию или в банк

- Если вы подозреваете, что от имени банка или компании вам звонят или пишут мошенники, прекратите общение и перезвоните в контактный центр, чтобы проверить информацию.
- Если подозреваете, что пароли или другие данные оказались доступны посторонним, немедленно смените пароли или блокируйте счёт.
- Если подозреваете, что ваше устройство кто-то использовал без вашего ведома, заблокируйте доступ в приложение или личный кабинет. Позвоните в компанию и отзовите скомпрометированный ключ электронной подписи.
- Если вы заметили несанкционированное движение ценных бумаг, денег и других финансовых активов на ваших счетах, срочно обратитесь в компанию.
- Звоните только на официальные телефоны компании и банка:

АО УК «Первая»
+7 495 5000-100
8 800 1003-111

ПАО Сбербанк
900
+7 495 500-55-50

Правила при использовании личного кабинета на сайте АО УК «Первая»

- Используйте на компьютере лицензионное программное обеспечение и вовремя его обновляйте.
- Составьте сложные пароли для доступа к компьютеру и личному кабинету. Пароли не должны содержать личную информацию, которую легко узнать (имя, фамилию или дату рождения), а также простые слова или наборы символов, которые легко подобрать, например: password или 1234567.
- Не храните пароли в открытом виде на компьютере или на мобильном устройстве.
- Не заходите в личный кабинет с чужих устройств: на них может быть установлен вредоносный код, собирающий пароли.
- Установите на компьютер антивирус, который регулярно и своевременно обновляется, а также файервол (брандмауэр, межсетевой экран) для фильтрации трафика и защиты данных от несанкционированного доступа злоумышленников.
- Ограничьте доступ к компьютеру посторонних людей, в том числе возможность дистанционного подключения.
- Не посещайте подозрительные сайты и не оставляйте на них персональную информацию.
- Не сохраняйте пароли в памяти браузера, если к компьютеру есть доступ у других людей.
- Не нажимайте на баннеры и всплывающие окна.
- Не открывайте файлы из неизвестных источников, особенно архивные файлы, поскольку они не всегда проверяются антивирусами автоматически.
- При работе с личным кабинетом, старайтесь не использовать публичные сети Wifi (кафе, общественный транспорт и т.п.).
- По окончании работы в личном кабинете, рекомендуем проводить очистку временных файлов и истории браузера, чтобы исключить несанкционированный доступ к Вашему личному кабинету.
-

Правила при использовании мобильных приложений АО УК «Первая» и Сбербанк Онлайн

- Используйте только официальные приложения управляющей компании и банка для iPhone, iPad и устройств на Android.
- Если доступ на мобильное устройство не закрыт паролем, установите его.
- Никому не сообщайте пароль для входа в мобильные приложения управляющей компании и банка.
- Установите в настройках безопасности устройства запрет на установку программ из неизвестных источников. Если у вас Android-устройство, не устанавливайте приложения, которых нет в Google Play.
- Своевременно обновляйте операционную систему устройства, особенно настройки

безопасности. Обновления снижают риск заражения вредоносным кодом.

- Не оставляйте без присмотра телефон или планшет, на который приходят СМС-коды и с которого вы входите в приложения АО УК «Первая» и

  Сбербанк Онлайн. Храните устройство так, чтобы посторонние не могли им завладеть.
- Если устройство окажется в чужих руках, злоумышленники могут воспользоваться им для доступа к вашему личному кабинету. Поэтому при утере или краже телефона сразу сообщите об этом по телефону компании (+7 495 5000-100) или телефону банка (900). На другом устройстве зайдите в приложение и смените пароль доступа в него. При возможности заблокируйте и перевыпустите сим-карту.
- Если сим-карта вышла из строя, сразу обратитесь к сотовому оператору, выясните причины и восстановите связь.
- Не используйте мобильное приложение на устройствах, на которых были повышены права доступа с применением неофициальных прошивок (root, jailbreak и т.п.).

При работе с ключами электронной подписи

- Если для входа в дистанционные сервисы пользуетесь квалифицированным сертификатом, используйте специальные защищенные носители для хранения ключей электронной подписи: e-token, ru-token, смарт-карту.
- Относитесь к носителю ключей электронной подписи очень внимательно, не оставляйте без присмотра и никому не передавайте. Извлекайте из компьютера, когда не используете.

Мы всегда на связи

Столкнулись с мошенниками? Срочно звоните:

+7 495 5000 100