

Правила безопасности при работе с сервисами Акционерного общества «Рублёво-Архангельское»

При работе с личным кабинетом Акционерного общества «Рублёво-Архангельское» помните, что защита вашей личной информации зависит в том числе и от вас!

Следуйте проверенным рекомендациям, тогда **ваша информация и доступ в личный кабинет** будут надёжно защищены:

- При работе с личным кабинетом используйте ПК или личное устройство **с установленным антивирусом** и ежедневно его **обновляйте**, регулярно **выполняйте проверку** ПК или устройства на наличие вирусов. Систематически **актуализируйте** операционную систему, приложения и программы — так разработчики устраняют уязвимости, которыми могут воспользоваться злоумышленники.
- Соблюдайте меры, **повышающие безопасность мобильного телефона** во время работы с личным кабинетом: не устанавливайте приложения из непроверенных источников. Пользуйтесь только **официальными магазинами** приложений (Google Play, AppGallery, AppStore, RuStore или NashStore). Не скачивайте и не устанавливайте **взломанные версии** приложений!
- Не работайте с личным кабинетом с использованием подключения к **общедоступным Wi-Fi-сетям**.
- Внимательно проверяйте **правильность адреса** личного кабинета: <https://sbercity.ru/personal>. Не вводите свои данные (логин и пароль) **при подозрении на мошеннический адрес**.

Внимание! В сети обнаружены не принадлежащие Акционерному обществу «Рублёво-Архангельское» сайты-клоны проекта Сберсити. Такие сайты могут содержать вирусы, вредоносные программы, а также собирать пароли пользователей от личного кабинета. В случае попыток авторизации в личном кабинете **на других ресурсах** рекомендуем **немедленно сменить пароль**, используя кнопку «Восстановить пароль» на экране авторизации.

Важно! Вход в личный кабинет Акционерного общества «Рублёво-Архангельское» возможен только через официальный сайт. У нас нет мобильного приложения для доступа в личный кабинет. Остерегайтесь подделок!

- **Не переходите по подозрительным ссылкам** из электронных писем, СМС-сообщений или сообщений из мессенджеров.

- Всегда делайте **надёжные пароли** для личных аккаунтов, составленные из парольных фраз и содержащие минимум 12 символов. **Чаще меняйте пароли** — рекомендуемый срок действия пароля не более 3 месяцев. **Не сообщайте свои логины и пароли** третьим лицам.

Важно! Надёжная защита возможна с использованием **двухфакторной аутентификации!** Раньше сервисы запрашивали только пароль, чтобы подтвердить вашу личность. Сейчас часто дополнительно просят ввести **одноразовый код** — это и есть «двухфакторная аутентификация». Обязательно **включайте двухфакторную аутентификацию везде, где это возможно**.



- При работе с личным кабинетом в общественных местах **исключайте подглядывание третьих лиц** в экран ПК или мобильного телефона — блокируйте экран ПК или мобильного устройства при прерывании работы с личным кабинетом.
- При поступлении **подозрительных звонков, СМС-сообщений, сообщений в соцсетях и мессенджерах** от имени Акционерного общества «Рублёво-Архангельское»:
 - Не перезванивайте на эти номера
 - Не сообщайте звонящим поступающие на телефон СМС-коды или какую-либо другую информацию
 - Прекращайте контакт и немедленно обращайтесь в Акционерное общество «Рублёво-Архангельское» по телефону +7 (495) 021-67-76
- **Никогда не храните на устройстве** логин и пароль доступа к личному кабинету Акционерного общества «Рублёво-Архангельское», банковским онлайн-приложениям, номера карт, паспортные данные и др. конфиденциальную информацию, чтобы она не стала доступна третьим лицам в случае утраты устройства.