ForteBusiness

Осторожно! Мошенники! Не дай себя обмануть!

Уважаемые клиенты Fortebank, в связи с участившимися случаями социальной инженерии напоминаем Вам основные рекомендации, как не стать жертвой мошенников:

01 Если Вам позвонили от имени Нацбанка или других Банков, Службы безопасности, прокуратуры, технической поддержки по поводу **«спасения Ваших денег», «восстановления доступа», «подтверждения Вашей личности»**, возьмите инициативу в свои руки – завершите звонок и самостоятельно свяжитесь с обслуживающим менеджером!

02 Никогда не сообщайте, не пересылайте **Ваши пароли и OTP-коды от** онлайн банкинга!

03 При получении реквизитов контрагента по почте, **перепроверьте полученную информацию по телефону!**

04 **Перепроверяйте информацию, полученную в мессенджерах,** особенно с неизвестных телефонов!

05 **Установите запрет на звонки** от неизвестных контактов или с иностранных номеров!

06 Учтите, что если Вы передаете функции проведения операций лицам, которые не внесены в учетные системы Банка, Вы повышаете риск финансовых потерь!

07 **Не передавайте Вашу компанию (юридическое лицо, ИП)** в аренду во избежание юридической и финансовой ответственности, в случае их неправомерного использования;

08 **Не сообщайте персональные данные или банковскую тайну (наличие счета, остатки, номера, реквизиты счета, карты)**, если есть сомнение в полномочиях или подлинности личности представителя банка или государственных органов;

09 **Соблюдайте меры кибергигиены и финансовой безопасности, рекомендованные физическим лицам и клиентам банка:**

- сохранение в тайне от третьих лиц учетных данных, паролей и логинов;
- должная осмотрительность при участии в инвестировании;
- использование проверенных, официальных сайтов и ссылок для осуществления покупок, заказов услуг;
- избежание сделок со 100% предоплатой по новым непроверенным реквизитам;
- избежание публичных WIFI сетей при проведении операций в Интернет и мобильном банкинге;
- исключение передачи третьим лицам, в т.ч. родственникам своих платежных инструментов и учетных данных;
- регулярное удаление из мессенджеров голосовых сообщений и иных биометрических данных, подробной информации о себе, друзьях и близких родственниках;
- исключение из использования программ удаленного пользования при осуществлении финансовых операций или оказание техпомощи от малознакомых лиц с использованием таких программ как AnyDesk, TeamViewer и др.

10 В случае подозрений на мошенничество или попытку мошенничества, незамедлительно обратитесь по номеру горячей линии **Банка 555-75.**

С подробной информацией можете ознакомиться на сайте **forte.kz**, также можете **просканировать QR** для перехода на сайт