ForteBusiness

Осторожно! Мошенники! Не дай себя обмануть!

Установите двухфакторную аутентификацию на все аккаунты (интернет-банкинг, почта, соцсети, мессенджеры и т.п.), которые вы используете.

При использовании интернет-банкинга **избегайте параллельной работы с другими интернет-сайтами**. Вначале обязательно завершите текущую сессию интернет-банкинга.

Избегайте работы с интернет-банкингом, если вы находитесь в публичном месте или используете открытые, общедоступные Wi-Fi сети. **Также не совершайте покупок и не передавайте критичную информацию** через почту или месседжеры.

Не пользуйтесь сайтами без сертификата безопасности (http). Убедитесь, что сайт защищен TLS шифрованием (слева от адресной строки должен отображаться закрытый замочек).

Не переходите по ссылкам, которые прислали по почте или в мессенджере малознакомые люди. Не открывайте письма или сообщения с незнакомых или подозрительных e-mail адресов. **Не загружайте и не открывайте вложения с таких писем. Не переходите по ссылкам в письмах, уведомляющих о получении наследства, приза.**

Не посещайте сайты сомнительного характера. Подобные ресурсы зачастую являются источниками вирусов.

Всегда проверяйте ссылку, по которой собираетесь кликнуть, не перепутаны ли буквы в названии или адресе сайта. Иногда фальшивые сайты полностью повторяют дизайн настоящих, но адрес ссылки точно будет отличаться от оригинала.

Не сканируйте QR коды, если не уверены в их подлинности. Перед оплатой покупки по QR убедитесь в уведомлении банковского приложения в подлинности продавца, покупки и оплачиваемой суммы.

Не выкладывайте в социальных сетях личную и корпоративную информацию с адресом, фотографиями, описанием проектов. **Не участвуйте в сетевых викторинах, играх, опросах, марафонах, требующих номер телефона, e-mail или иную личную информацию.** Установите в социальных сетях настройки приватности. Например, закрыть/ограничить комментирование, просмотр фотографий.

В случае появления каких ли нестандартных сообщения, аномальной или необычной работы устройства, неуместно появляющихся окон, в которых запрашивается ваши пароли, пины или OTP коды - **незамедлительно отключите устройство и свяжитесь с обслуживающим менеджером.**

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