Пользователю Интернет банкинга необходимо использовать следующие меры безопасности:

· обеспечить режим конфиденциальности в отношении своего рабочего места, логинов и паролей в Интернет Банкинг;
· входить в личный кабинет Интернет Банкинга https://www.online.fincabank.kg / только по ссылке с официального сайта Банка (www.fincabank.kg). Перед входом в систему, убедиться в безопасности веб-страницы, проверив наличие Унифицированных Указателей Ресурсов (URL), которые должны начинаться с «https», а на статусе интернет-браузера должен появиться знак защищённого соединения;
· не сохранять пароль в текстовых файлах на компьютере, либо на других носителях информации;
· не раскрывать логины и пароли третьим лицам, включая сотрудников Банка (в том числе при обращении неустановленных лиц от имени Банка по телефону, электронной почте, через SMS). Пароль не требуется сотрудникам Банка и службе технической поддержки для подключения, обслуживания и поддержки сервиса в работоспособном состоянии;
· после окончания работы в системе Интернет Банкинг корректно завершать работу с использованием программной кнопки «Выход».
· не использовать рабочее место для подключения к социальным сетям в сети Интернет, к форумам, конференциям, чатам, телефонным сервисам и иным сайтам, содержащим потенциальные вредоносные программы, а также для чтения почты и открытие почтовых документов от адресатов, незаслуживающих доверия;
· использовать для работы с системой Интернет Банкинг выделенное рабочее место, не используемое Пользователем в других целях;
· обеспечить функционирование на рабочем месте Пользователя лицензионной версии (не контрафактной) операционной системы Microsoft Windows XP/2003/Vista/7, Apple Macintosh Mac OS X или старше, Linux и её своевременное обновление согласно 10 рекомендациям компании-разработчика в целях устранения, выявленных в ней уязвимостей, позволяющих получить доступ к конфиденциальной информации;
· обеспечить функционирование на рабочем месте Пользователя лицензионного (не контрафактного) антивирусного программного обеспечения и его своевременное обновление согласно рекомендациям компании-разработчика. Это требуется в целях недопущения заражения рабочего места пользователя вредоносным программным обеспечением, способным предоставить несанкционированный доступ неуполномоченным третьим лицам в Интернет Банкинг от имени Пользователя;
· обеспечить функционирование на рабочем месте лицензионного (не контрафактного) программного обеспечения «брандмауэр (firewall)» в режиме блокирования несанкционированного удалённого доступа к рабочему месту из сети Интернет и локальной сети Пользователя;
· ограничить доступ к персональному компьютеру и обеспечить наличие минимальных прав для изменения конфигурации операционной системы рабочего места Пользователя (наличие прав администратора нежелательно);

· не работать в системе Интернет Банкинг в сети Интернет, используя источник подключения из мест, не заслуживающих доверия (интернет-кафе), или используя общественные каналы связи (бесплатный Wi-Fi и т.п.);
· обращать внимание на любые изменения и ошибки программного обеспечения во время установления соединения в системе Интернет Банкинг Банка или в работе Интернет Банкинга, при возникновении любых сомнений в правильности работы Интернет Банкинга незамедлительно прекратить работу и обратится в Банк в целях установления отсутствия/наличия несанкционированные операций;
· в случае появления предупреждений браузера о перенаправлении на другой сайт при подключении к системе Интернет Банкинг, отложить совершение операций и обратиться в отдел поддержки клиентов (0312 440-440) Банка в целях установления причины перенаправления;
· регулярно проверять историю операций и выписки для отслеживания ошибок или неавторизированных операций по счету;
· не покидать сайт, где осуществляются электронные операции, даже если персональный компьютер оставлен без присмотра на короткий срок.