РЕКОМЕНДАЦИИ КЛИЕНТАМ
по соблюдению мер информационной безопасности
при использовании информационных ресурсов
ООО «Пермская фондовая компания».

Рекомендации по защите информации от воздействия вредоносного кода и по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления.

Риски получения негативного воздействия вредоносного кода и несанкционированного доступа к информации, прежде всего, связаны с «фишингом» и «троянами».

«Трояны» - специализированные вредоносные программы для похищения личных данных пользователей и их незаконного использования для выполнения несанкционированных операций от имени клиента. Трояны распространяются по электронной почте, по каналам сервисов мгновенной передачи информации и через принадлежащие злоумышленникам сайты.

«Фишинг» – попытка перехвата личных данных клиента. Один из самых распространенных способов фишинга - отправка электронных писем мошенниками, которые выдают себя за представителей известной компании. Как правило, в таких электронных письмах содержится ссылка на небезопасную страницу web-сайта. На этой странице Вам предлагается ввести свои личные данные, при этом Вы можете полагать, что ввод данных безопасен, тогда как в действительности информация похищается злоумышленниками.

Оптимальный способ защиты от кражи учетных данных состоит в умении распознавать способы этих злоумышленных действий и предотвращении таких ситуаций:

- При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.
- Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.
- Своевременно обновляйте установленное программное обеспечение и операционную систему.
- Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов.
- При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.
- При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ.
- Исключите возможность установки посторонними лицами (гостями, посетителями) на Ваш компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.
- Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто, в виде «интересной ссылки» в письме, от якобы знакомого, приходит вредоносная программа. Зачастую вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.
- - При подозрениях на наличие вирусов на персональном компьютере (например, неожиданных «зависаниях», перезагрузках, сетевой активности), рекомендуем полностью воздержаться от использования информационных систем до исправления ситуации.