Рекомендации по обеспечению информационной безопасности для клиентов общества с ограниченной ответственностью «Все инвестиции»

Уважаемые клиенты!

ООО «Все инвестиции» доводит до вашего сведения информацию о рисках, которые возникают при совершение финансовых операций в информационно -телекоммуникационной сети «Интернет» (далее –Интернет) и о необходимых мерах безопасности, которые помогут вам в защите ваших данных и денежных средств.

Основные риски:

При работе в сети Интернет стоит опасаться кражи денежных средств, а также ваших пользовательских данных: логинов, паролей, PIN-кодов, паспортных данных и пр. Такие операции зачастую происходят по следующим причинам:

мошенники могут получить контроль над вашими устройствами, такими как компьютер, ноутбук, планшет, мобильный телефон, с которых вы подключаетесь к личному кабинету, мобильному приложению или интернет-банку для совершения финансовых операций;

мошенники будут пытаться осуществить списание денежных средств в свою пользу, проведение операций с доступными активами, подключение и отключение услуг (в том числе платных), внесение изменений в данные, указанные вами в личном кабинете, мобильном приложении или интернет-банке.

мошенники могут вывести из строя ваше устройство, что в свою очередь грозит невозможностью своевременного исполнения ваших обязательств по договору, а также недоступностью необходимых финансовых сервисов.

Вышеуказанное может происходить как с использованием вирусов (вредоносных программ), так и с помощью психологических манипуляций, когда мошенник получает доступ к вашим персональным данным или денежным средствам.

Общие рекомендации, которые помогут вам в защите ваших данных и денежных средств:

Если вам звонит «представитель» нашей компании либо «службы безопасности», «специалист технической поддержки» банка и т.п. и побуждает к каким-либо конкретным действиям с вашими денежными средствами, или даже просит доверить ему управление операциями по счету, необходимо незамедлительно прервать разговор и перезвонить по номеру телефона, указанному на официальном сайте финансовой организации. Помните: официальные представители владеют всей необходимой информацией о ваших счетах и платежной карте и никогда не запрашивают реквизиты карт, логины и пароли по телефону или через интернет. Они могут лишь рекомендовать вам определенные действия, как владельцу денежных средств.

Не сообщайте посторонним лицам информацию, которая используется вами для совершения любых финансовых операций. Наиболее ценны для мошенников ваши персональные данные, данные банковских карт, пароли из SMS и push-уведомления, подтверждающие финансовые операции, а также кодовые слова, указанные вами в анкете финансовых организаций и т.д.

Используйте сложные пароли и одноразовый код подтверждения в виде SMS или push-уведомлений для входа в личный кабинет, мобильное приложение или интернет-банк финансовой организации или дополнительную защиту PIN-кодом финансового приложения на вашем телефоне. Чем сложнее пароль, тем труднее мошенникам его подобрать.

Не подключайтесь к личному кабинету, мобильному приложению или интернет-банку для совершения финансовых операции с любых других устройств, кроме ваших.

Не используйте функцию запоминания логина и пароля, номера карты, кодов доступа и пр. при работе в сети Интернет.

Обращайте внимание на всплывающие окна на сайтах с сообщениями о том, что сайт ненадежный или подключение не защищено. Надежность таких сайтов для проведения финансовых операций должна вызывать сомнение.

Не рекомендуем регистрироваться в социальных сетях, интернет-магазинах и на других ресурсах с номера вашего мобильного телефона, который привязан к личному кабинету, мобильному приложению или интернет-банку.

Не открывайте ссылки и вложения от неизвестных отправителей в электронной почте, SMS, мессенджерах). В них могут содержаться ссылки на мошеннические сайты–двойники. Безопасные веб-сайты отмечены значком в виде закрытого замка, адрес сайта должен начинаться с https://. Письма, содержащие архивы с паролем, зашифрованные файлы, где в содержании этого же письма указан и пароль, очень часто содержат вирусы.

Скачивайте и устанавливайте приложения на мобильные телефоны и планшеты только из Google Play, AppStore, Huawei AppGallery и других официальных магазинов мобильных приложений.

Устанавливайте лицензионное антивирусное программное обеспечение, периодически обновляйте антивирусные базы и проводите полную антивирусную проверку устройств.

Рекомендации по использованию парольной защиты:

Постарайтесь запоминать свои пароли. Используйте сложные и разные пароли к сайтам и приложениям, требующие ввода заглавных и прописных букв, цифр и специальных символов в общем количестве не менее восьми символов (например, GH&^12#$B). Не рекомендуется в качестве паролей использовать осмысленные слова, повторяющиеся символы, имена близких людей, домашних животных, даты рождения, которые могут быть легко подобраны мошенниками (например, qwerty, 789456, abcdefgh).

Не сохраняйте пароли в текстовых файлах на устройстве в открытом виде. Для безопасного хранения паролей рекомендуется использовать специализированные программы.

При смене пароля используйте совершенно новый вариант, полностью отличный от предыдущего.

Никому, в том числе родственникам, друзьям, работникам банков и других организаций, не передавайте ваши логины и пароли, PIN-коды и иные данные, используемые для проведения финансовых операций.

В случае утраты или кражи устройства, на которое вам направляются одноразовые пароли или подключена услуга SMS-информирования, незамедлительно заблокируйте SIM-карту, смените пароли доступа в финансовых приложениях. Также полезно использовать функцию удаленной блокировки — это дает возможность заблокировать устройство, ограничить его работоспособность и/или стереть все ваши данные при утрате или краже устройств.

Используйте дополнительный пароль или код для доступа к вашему устройству. Напоминаем, что использование Face Unlock, Face ID или Touch ID не гарантируют абсолютную безопасность ваших данных.

Рекомендации при работе в сети Интернет:

Будьте осторожны при использовании Wi-Fi-сетей в кафе, ресторанах, отелях и других общественных местах. Мошенники научились создавать фальшивые Wi-Fi-сети для перехвата логинов и паролей.

Не сохраняйте, не скачивайте и не устанавливайте подозрительные файлы, программы, полученные из ненадежных источников (с неизвестных сайтов, присланные с неизвестных адресов электронной почты, по ссылкам через SMS или мессенджеры).

Проявляйте внимательность при переходе по ссылкам и нажатии на кнопки во всплывающих окнах браузера — они могут вести на мошеннические ресурсы.

Особенно внимательно проверяйте наименование сайта. Часто мошенники создают копию официального сайта компании, меняя одну букву в названии. Используя такие сайты-двойники, мошенники могут получать доступ к вашим пользовательским данным и денежным средствам.

После окончания работы в личном кабинете на сайте завершайте сеанс, используя кнопку «Выход».

ВНИМАНИЕ:
Распространенным видом мошенничества является «фишинг». Он подразумевает получение мошенниками обманным путем ваших логинов и паролей, номера счета, PIN-кода, кода доступа,

CVC\CVV кодов и т.д. с помощью создания поддельных сайтов, полностью копирующих сайты банков и других организаций, и поддельных информационных рассылок, где вам предлагается пройти по ссылке на эти сайты.

Напоминаем, сотрудники нашей компании и других учреждений никогда и ни при каких обстоятельствах не запрашивают:

- логин и пароль для входа в мобильный и интернет-банк;
- содержание одноразовых кодов подтверждения;
- номера счетов и банковских карт;
- CVC/CVV-коды;
- дату окончания срока действия банковской карты.

Также сотрудники никогда не просят установить сторонние программы удаленного доступа. Все это признаки того, что с вами связались мошенники.

Рекомендуем порядок действий в случае подозрений на несанкционированный доступ к вашим данным:

Если раскрыты логины и пароли в личный кабинет или другие персональные данные, свяжитесь с компанией, данные которой были скомпрометированы, и сообщите о мошенничестве. Также можно заблокировать все возможные действия по вашим счетам.

Если устройство заражено вирусом обратитесь в сервисный центр, который рекомендует производитель.

Если возникли подозрения на кражу пароля, как можно быстрее смените его.

В случае подозрения на мошенничество от лица ООО «Все инвестиции» незамедлительно свяжитесь с нашими специалистами по телефону: 8 (495) 745 85-00 или по электронной почте info@allinpower.ru сообщите об инциденте.

Официальный сайт компании находятся по адресу: https://allinpower.ru/.