High Yield Investment Program (ХАЙП)

Part #1 : Clarification (Russian)
Part #2 : Security (Russian)
Part #3 : Investing (Russian)

Part #2 : Security (Russian)

Безопасность при работе с электронными платежными системами

Ни одна электронная платежная система, сколь бы она надежна ни была, не может вам гарантировать стопроцентную защищенность от несанкционированного доступа. Лишь только соблюдая правила безопасности, можно добиться сохранности денежных средств. Огромное количество взломов совершается из-за разгильдяйства и невнимательности самих владельцев аккаунтов. Существует ряд правил, неукоснительно следование которым поможет пользователям максимально оградить себя от мошенников.

1. Операционная система Windows предлагает пользователю функцию автозаполнения паролей. Несмотря на то, что при работе с некоторыми ресурсами данная опция может оказаться достаточно полезной, ее категорически не рекомендуется использовать при доступе к аккаунтам электронных платежных систем. Иначе злоумышленнику не составит никакого труда похитить ваши регистрационные данные и затем опустошить ваш электронный кошелек.
2. Все специальные файлы, которые нужны для работы с некоторыми электронными платежными системами, необходимо хранить на дискетах или на зашифрованных дисках, доступ к которым должен предоставляться только в момент начала работы с кипером.
3. Никогда не открывайте электронную почту, присланную с незнакомых вам адресов. В подобных письмах могут находиться вирусы и Трояны, с помощью которых злоумышленники способны похитить логин и пароль от вашего аккаунта. Установите почтовую программу, позволяющую обезвреживать электронные письма с потенциально опасными вложениями, проверяйте входящие сообщения с помощью специальных антивирусов.
4. Никогда не переходите по ссылкам, которые присылают вам незнакомые люди. В том случае, если вы оказались на незнакомой интернет-странице, ни в коем случае не заполняйте там никаких полей и не проходите процедуру регистрации. Ни в коем случае не соглашайтесь скачивать программное обеспечение, которое вам будут навязчиво предлагать. Многие из подобных страниц создаются для того, чтобы всучить клиенту программу-шпион.

5. На вашем персональном компьютере всегда должна быть установлена программа-антивирус и файрволл. Использование данных программных средств поможет минимизировать вероятность атаки извне. Антивирус защитит вас от вредоносных программ, а файрволл даст возможность отбиться от хакерских атак.
6. Не обращайте внимания на письма, которые подписаны службой технической поддержкой используемой вами электронной платежной системы. Как правило, их рассылают злоумышленники, рассчитывая на то, что хозяева аккаунтов, поверив в правдивость присланной информации о якобы имевших место проблемах с функционированием системы, отошлют на фиктивный адрес свои регистрационные данные, логин и пароль. Если вы не уверены в том, что с вами связываются представители службы технической поддержки, лучше напишите на официальный адрес письмо и уточните детали. Скорее всего вам ответят, что никогда и никому сообщений с требованием выслать пароль не отсылали, а с вами пытались связаться обычные мошенники.
7. Никогда не скачивайте программы, предназначенные для взлома чужих электронных кошельков или увеличения количества денег на своих счетах. Подобных приложений **не существует**, под их видом злоумышленники рассылают Троянов. Вместо генерации на счете дополнительных средств, вы, скорее всего, просто потеряете свои сбережения. Создатели электронных платежных систем крайне серьезно подходят к вопросу обеспечения безопасности своих кошельков и с помощью маленького приложения, написанного программистом-любителем их взломать невозможно. Зато можно похитить логин и пароль у пользователя, решившего нажиться за чужой счет.
8. Как минимум раз в неделю меняйте все свои пароли. Даже если злоумышленнику и удалось получить доступ к вашему аккаунту, то, сменив пароль, вы лишите его возможности распоряжаться денежными средствами на вашем счете.

Кроме того, не забывайте об очевидных методах сохранения конфиденциальности информации. Например, не стоит записывать пароль доступа к счету электронной платежной системе на бумажку, а потом оставлять ее на видно месте. Пароль не должен быть простым и очевидным, не стоит использовать свой год рождения, домашний телефон или имя. Самый лучший пароль – бессвязный набор букв и цифр. Подобрать его сложнее всего, а угадать – практически невозможно.

Соблюдение этих несложных правил поможет вам избежать неприятных ситуаций и надежно защитить свои электронные сбережения от воров.