Памятка о безопасном использовании

Основные правила, которые помогут защититься от мошенников:

1. Проверяйте сайты, на которых вводите логин и пароль от аккаунта и другую конфиденциальную информацию.

Основной прием хищения конфиденциальных клиентских данных — их сбор на поддельных ресурсах.

Фишинговый сайт — поддельный сайт, который выглядит как реальный ресурс, но используется для сбора конфиденциальной информации.

Попасть на такие ресурсы можно, если перейти по ссылкам из SMS, электронных писем, сообщений в мессенджерах и соцсетях, а иногда по рекламным ссылкам или ссылкам из топа поисковиков.

Для доступа в веб-версию приложения Яндекс Финансовая Платформа используйте только ресурс https://finance.yandex.ru/.

2. Устанавливайте приложения только из официальных магазинов приложений: App Store, Google Play и других.

Общайтесь с нами только через официальные приложения Яндекса.

Не устанавливайте «обновления», о которых вас просят на сайтах или в SMS, в сообщениях в соцсетях и мессенджерах.

3. Яндекс Финансовая Платформа не просит устанавливать дополнительные приложения!

Одна из уловок мошенников — под видом системы защиты или антивируса просят установить TeamViewer, AnyDesk и другие приложения для удаленного доступа.

С их помощью мошенник сможет читать направленные вам сообщения и даже полностью управлять телефоном.

4. Установите двухфакторную аутентификацию.

Для входа в приложение используйте двухфакторную аутентификацию — дополнительный уровень безопасности надежнее защитит аккаунт от несанкционированного доступа.

5. Чаще меняйте пароли.

Рекомендуем менять пароль не реже раза в полгода.

Чтобы пароль был надежным, придерживайтесь рекомендаций:

— минимальная длина 10–12 символов;

— содержит цифры, спецсимволы и буквы в разном регистре (! @ _ %);

— не используйте личные данные: логин, дату рождения, номер телефона;

— не задавайте простые последовательности (123456789, qwerty, zaqxsw).

Полные рекомендации по защите вашего аккаунта описаны в Справке.

6. Включите PIN-код на SIM-карте.

Установите PIN-код на вашей SIM-карте, чтобы в случае утери ее не смогли использовать на другом устройстве, например, для получения SMS для входа в приложение или подтверждения операций по карте.

7. Знакомый попросил вас перевести ему денег? Убедитесь, что это точно он.

Если знакомый из списка контактов в соцсети прислал вам сообщение с просьбой о переводе денег, не переводите их, пока не убедитесь, что просит знакомый, а не мошенник. Прежде чем перевести деньги, позвоните по телефону или свяжитесь с вашим знакомым любым другим способом, но не через ту соцсеть, по которой вы получили сообщение.

8. Эти данные должны знать только вы:

— логин и пароль от приложений Яндекса;

— коды и пароли из SMS и пуш-уведомлений для подтверждения оплаты;

— реквизиты карты: срок действия и CVV. Для перечисления вам средств достаточно ТОЛЬКО номера карты!

— ПИН-код от карты (не сообщайте его третьим лицам и даже родственникам).

Сотрудники банков или Яндекс Финансовая Платформа никогда не спросят эти данные! Если спросили, значит, вы разговариваете с мошенником. Положите трубку и свяжитесь с нами.

9. Установите на телефоне режим, не позволяющий читать сообщения и уведомления на заблокированном устройстве.

10. Для оплаты на торговых площадках (Авито, Юла и других) используйте официальные сервисы. Не оплачивайте по ссылкам, полученным в мессенджерах или в чате данных площадок.

11. Нашли в интернете нужный товар/услугу по нереально низкой цене или с огромной скидкой? Проверьте ресурс: скорее всего, это мошенничество.

12. Есть сомнения? Пишите в поддержку вашего банка!

Входящий звонок с любого номера может принадлежать мошенникам. К сожалению, они могут подменить номер. Если сомневаетесь, положите трубку и перезвоните сами.