

МОШЕННИЧЕСТВО ПОСРЕДСТВОМ ФИШИНГОВЫХ САЙТОВ И САЙТОВ-ПОДДЕЛОК

КГБУ СО
«КЦСОН «Бирюлюсский»

Цель: получить доступ к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, образовательных организаций, а также личных сообщений внутри различных сервисов или социальных сетей. В письме часто содержится прямая ссылка или баннер, ведущий на сайт, внешне не отличимый от настоящего.

ВАЖНО:

1. Если при переходе на посещаемый вами сайт или сервис по ссылке, полученной в мессенджере или по электронной почте, браузер просит вновь ввести логин и пароль для входа — стоит обратить пристальное внимание на название сайта в адресной строке.
2. Для того, чтобы обезопасить доступ к персональному аккаунту в социальных сетях, настоятельно рекомендуется установить двухфакторную аутентификацию - таким образом при входе в аккаунт с нового устройства вам на телефон будет приходить смс с кодом подтверждения.
3. При совершении покупок в онлайн-магазинах, особенно не проверенных брендов и сервисов, не регистрируйтесь посредством своего аккаунта в социальных сетях — лучше создать новую учетную запись.
4. При оплате банковской картой в онлайн магазине, старайтесь совершать это в безопасном режиме. Чаще всего браузер предложит им воспользоваться автоматически, если нет, это может служить поводом насторожиться.

МОШЕННИЧЕСТВО С ПОМОЩЬЮ САЙТОВ



Новобирюлюссы
2022 г.

ОСНОВНЫЕ СОВЕТЫ ПО БОРЬБЕ С

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

ПЕРЕВОД ДЕНЕЖНЫХ СРЕДСТВ НА

ФИШИНГОМ (ИНТЕРНЕТ-МОШЕННИЧЕСТВО):

- Следите за своим аккаунтом. Если вы подозреваете, что Ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используйте сложные и разные пароли. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному Вашему профилю в сети, а не ко всем;
- Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у Вас в друзьях, о том, что Вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установите надежный пароль (PIN) на мобильный телефон;
- Отключите сохранение пароля в браузере.

БАНКОВСКИХ ПРИЛОЖЕНИЙ:

- Не указывать номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах социальных сетей (одна sim-карта для общения, вторая для сервисов, связанных с банками и государственными услугами);
- При заключении договора с банком уточнить возможность указать в договоре, либо в иной форме согласовать с банком, что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, ограничить круг операций, установить лимит денежных средств, который можно переводить с помощью мобильного устройства;
- Запретить перевод всего объема денежных средств с карты, счета — установите лимит.

БЛАГОТВОРИТЕЛЬНОСТЬ, СРОЧНАЯ ПРОСЬБА О ПОМОЩИ БЛИЗКОГО ИЛИ ЗНАКОМОГО ЧЕЛОВЕКА С ЕГО СТРАНИЦЫ.

1. Если вы хотите участвовать в благотворительности, это лучше всего делать через проверенные организации. В социальных сетях чаще всего собирают денежные средства мошенники.
2. Если сообщение в социальной сети о просьбе помочь Вас действительно затронуло обратите внимание на следующие обстоятельства перед переводом денежных средств: соответствует ли фамилия и город проживания с указанными реквизитами получателя, если есть упоминания о предыдущем сборе средств в сети, через поисковые системы проверьте фотографии на предмет их уникальности.
3. В случае финансовой просьбы о помощи Вашего близкого обратите внимание: указана ли цель просьбы, может ли человек назвать какие-то факты известные только вам, не поленитесь позвонить и лично уточнить ситуацию.