

Профилактика IT-преступлений

В целях профилактики IT-преступлений ГУ МВД России по Кемеровской области - Кузбассу подготовило информационные материалы по предотвращению (предупреждению) мошенничества в сети «Интернет»: памятки, видео материалы, буклеты, плакаты, аудио материалы.

Указанные материалы размещены по адресу:
<https://cloud.mail.ru/public/EiPJ/q25k6Xezv>.

Пожалуйста, ознакомьтесь с материалами. И будьте бдительными при получении смс-сообщений, электронных писем, каких-либо других обращений к вам подозрительного характера.

Имейте также в виду, что для осуществления своей преступной деятельности мошенники используют социальные сети, а также создают для этих целей интернет - магазины. Участие в подобных схемах подразумевает наличие всевозможных рисков и привлекает лиц, имеющих намерения на противоправное завладение денежными средствами граждан.

В связи с этим обращаем внимание, что интернет - ресурсы могут быть зарегистрированы с помощью зарубежных сайтов, предоставляющих услуги анонимизации, что не позволит в ряде случаев пользователю установить достоверные сведения о лицах, которым он доверил денежные средства.

Будьте внимательны и осторожны.

Некоторые плакаты представлены ниже.

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ
ЗАПОМНИТЬ ОСНОВНЫЕ СХЕМЫ И
ПРИЗНАКИ МОШЕННИЧЕСТВ!

Покупка либо продажа

товаров через сайты объявлений

ПРИЗНАКИ:

- Низкая стоимость товара;
- Требование безналичного расчета;
- Предложение подключить «мобильный банк»;
- Собеседник просит назвать реквизиты банковской карты и пароли из СМС-сообщений;
- Продавец под разными предлогами просит внести предоплату;
- Покупатель готов сделать покупку, даже не взглянув на нее.

РЕКОМЕНДАЦИИ:

- Для получения денежного перевода покупателю достаточно знать только номер Вашей банковской карты! Никогда не называйте пароли, приходящие от банка по СМС!
- Главная цель злоумышленников – подключиться к Вашему «мобильному банку»!
- Если услышали от покупателя предложение пройти к банкомату для получения перевода, знайте: Вас пытаются обмануть!

Компенсация

за приобретенные лекарства (БАДы)

ПРИЗНАКИ:

- Поступление телефонных звонков, начинающихся преимущественно с цифр «8-495...», «8-499...», «8-812...»;
- Собеседник представляется работником правоохранительных органов и сообщает, будто Вам полагается компенсация за ранее приобретенные медицинские препараты или БАДы;
- Собеседник пытается убедить Вас, что для получения денег необходимо оплатить НДС, страховку и т.д.

РЕКОМЕНДАЦИИ:

- Запомните: компенсация за ранее приобретенные лекарства или БАДы является стандартной уловкой мошенников!
- Не приобретайте медицинские препараты или добавки через Интернет и не заказывайте их по телефону. Любой курс терапии назначается только лечащим врачом!
- Не переводите деньги по просьбе знакомцев, кем бы они ни представлялись!

«Родственник в беде»

ПРИЗНАКИ:

- Неизвестный звонит на телефон, представляется, как правило, сыном или внуком и говорит, будто совершил ДТП или преступление, в результате которого пострадал человек;
- Собеседник передает телефонную трубку якобы сотруднику правоохранительных органов, который пытается убедить Вас, что для изъятия родственника от уголовного преследования необходимы деньги;
- Собеседник пытается удержать Вас на связи любыми способами, чтобы не дать возможность поговорить с родными.

РЕКОМЕНДАЦИИ:

- Задайте собеседнику вопрос, ответ на который знает только близкий Вам человек.
- Прервите разговор и перезвоните родным, чтобы убедиться, что с ними все в порядке!
- Если собеседник представляется работником правоохранительных органов, попросите его назвать фамилию, имя, отчество, а также должность и место службы. Позвоните в соответствующее ведомство и узнайте, действительно ли в нем работает такой сотрудник.
- Помните, что передача денежных средств должностным лицам за незаконные действия или бездействия является уголовно наказуемым деянием.

Взлом

(дублирование) страниц пользователей
в социальных сетях

ПРИЗНАКИ:

- В социальной сети от пользователя из списка Ваших друзей поступает сообщение с просьбой одолжить денежные средства либо предложением принять участие в акции банка и получить гарантированный денежный приз;
- Под этими предлогами собеседник просит назвать реквизиты банковской карты и пароли из СМС-сообщений.

РЕКОМЕНДАЦИИ:

- Отличить настоящую страницу пользователя в соцсети от ее дубликата, созданного мошенниками, внешне практически невозможно! Поэтому обязательно перезвоните человеку, от имени которого Вам поступило сообщение, и уточните достоверность информации.
- Помните: реквизиты банковской карты являются конфиденциальной информацией ее владельца, как и уведомления банка с паролями, необходимыми для подтверждения той или иной операции.
- Защитите от взлома свои аккаунты в социальных сетях при помощи надежного пароля, который необходимо держать в тайне от окружающих.

Маскировка

номера мошенника под телефон
«горячей линии» банка

ПРИЗНАКИ:

- Поступление телефонного звонка от «специалиста» либо «сотрудника службы безопасности» с номера «горячей линии» банка (8-800...) либо с незнакомых номеров, начинающихся на 8-495..., 8-499...;
- Сообщение о попытке оплаты товаров либо списания денежных средств с Вашего счета;
- Предложение назвать поступившие посредством СМС-уведомлений логины и пароли, а также срок действия, номер Вашей банковской карты и защитный код к ней, расположенный на обратной стороне платежного средства.

РЕКОМЕНДАЦИИ:

- Никогда, никому и ни под какими предлогами не называйте поступившие посредством СМС-уведомлений логины и пароли а также срок действия, номер Вашей банковской карты и защитный код к ней, расположенный на обратной стороне платежного средства;
- Помните, что получение конфиденциальной информации под предлогом защиты от неправомерного списания денег является стандартной мошеннической схемой!

Вирусы

распространение вредоносного
программного обеспечения

ПРИЗНАКИ:

- На телефон поступает сообщение от абонента из списка контактов в Вашей телефонной книге с предложением открыть прилагаемую интернет-ссылку, чтобы, например, посмотреть фото;
- Если Вы откроете ссылку, Ваш телефон может перезагрузиться или вовсе выйти из строя.

РЕКОМЕНДАЦИИ:

- Ни в коем случае не открывайте интернет-ссылки, полученные по смс или в мессенджерах даже от собственных знакомых! Пройдя по ним, можно загрузить вредоносную программу в свой мобильный телефон. Если сим-карта подключена к Вашему «мобильному банку», произойдет списание денег со счета.
- Зараженный телефон может автоматически рассылать аналогичные ссылки всем абонентам из списка контактов в Вашей телефонной книге.



ПОЛИЦИЯ КУЗБАССА ПРЕДУПРЕЖДАЕТ

ОСТОРОЖНО!

МОШЕННИКИ!



Звонок от «сотрудника банка»



ПРИЗНАКИ

- 1** поступление звонка от «сотрудника банка» (специалиста, работника службы безопасности);
- 2** сообщение о попытке хищения денежных средств; предложение заблокировать несанкционированную операцию либо перевести денежные средства на «безопасный» счет;
- 3** просьба назвать реквизиты банковской карты, защитный код с ее обратной стороны и поступающие на телефон пароли.

ЗАПОМНИТЕ!



НЕ ОТВЕЧАЙТЕ НА ЗВОНКИ, поступившие с неизвестных номеров, особенно зарегистрированных в другом регионе;



НЕ ВЕРЬТЕ любой информации от незнакомца, **ДАЖЕ ЕСЛИ** звонок поступил с официального телефона горячей линии банка;



ПРЕРВИТЕ РАЗГОВОР и самостоятельно позвоните на телефон горячей линии банка, набрав номер **ВРУЧНУЮ**;



ПОМНИТЕ: код от вашей карты и пароли подтверждения операций **НЕ ИМЕЕТ ПРАВА** спрашивать даже сотрудник банка!



42.мвд.рф



ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Запомните основные схемы и признаки популярных мошенничеств!
Эта информация поможет вовремя распознать злоумышленников.



Взлом (дублирование) страниц пользователей в СОЦИАЛЬНЫХ СЕТЯХ

ПРИЗНАКИ

- 1** В социальной сети от пользователя из **списка Ваших друзей** поступает сообщение с **просьбой одолжить денежные средства** либо предложением **принять участие в акции** банка и получить гарантированный денежный приз
- 2** Под этими предложениями собеседник просит назвать **реквизиты банковской карты и пароли из СМС-сообщений**

ЗАПОМНИТЕ:



Отличить настоящую страницу пользователя в соцсети **от ее дубликата**, созданного мошенниками, внешне практически **невозможно!** Поэтому обязательно **перезвоните человеку**, от имени которого Вам поступило сообщение, и уточните достоверность информации.



Реквизиты банковской карты являются конфиденциальной **информацией ее владельца**, как и **уведомления банка с паролями**, необходимыми для подтверждения той или иной операции.



Защитите от взлома свои аккаунты в социальных сетях при помощи **надежного пароля**, который необходимо держать **втайне** от окружающих.



42.мвд.рф