

Киберпреступность в Кузбассе

Почти ежедневно жители Кемеровской области становятся жертвами киберпреступников. С начала 2020 года полиция региона зарегистрировала почти 4000 онлайн-краж и мошенничеств. Стражи порядка констатируют, что аферисты постоянно изменяют схемы обмана и придумывают новые способы отъема денег у населения. При этом потерпевшие не только теряют свои накопления, но и невольно становятся заемщиками крупных банковских займов – до нескольких миллионов рублей.



ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

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

Преступления, совершаемые лицами ЦЫГАНСКОЙ народности

ПРИЗНАКИ

- 1 Попытка попасть в ваше жилище под видом работника ЖКХ, врача или сотрудника социальных служб, а также под предлогом покупки жилья, предоставления ночлега
- 2 Предложение обмена «старых» денег на «новые» или получения доплат к пенсии
- 3 Предложение купить дешевые мед, посуду, уголь, одежду
- 4 Предложение снятия «порчи», проведение ритуалов с использованием швейных игл, куриных яиц, «червей», «живой» или святой воды
- 5 Просьба одолжить деньги якобы для оформления груза на таможне, обещание вернуть долг «с процентами»

ЗАПОМНИТЕ:

-  Никогда не открывайте дверь незнакомцам и не впускайте посторонних в свою квартиру или дом!
-  Не показывайте и не передавайте деньги и ювелирные украшения посторонним!
-  Избегайте общения с теми, кто предлагает купить дешевые товары или продукты питания, погадать либо снять порчу!
-  Обращайте внимание на денежные купюры, получаемые из рук незнакомцев. Надпись «Купюра банка приколов» означает, что она сувенирная!

 42.мвд.рф

ГУ МВД России по Кемеровской области составило список городов, жители которых чаще всего становятся жертвами киберпреступлений. Большая часть зарегистрированных в регионе мошенничеств и краж, совершаемых с использованием IT-технологий, приходится на Кемерово (960 фактов) и Новокузнецк (848 случаев). Далее идет Прокопьевск,

Ленинск-Кузнецкий, Белово, Киселевск, Юрга, Анжеро-Судженск и Мыски. На них в общей сложности приходится более 1000 онлайн-хищений. Общая сумма причиненного потерпевшим ущерба составила около 240 миллионов рублей.



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**

Полицейские отмечают, что более половины жертв сетевых краж и мошенничеств – трудоустроенные граждане (более 54%), еще 27,5% приходится на пенсионеров и инвалидов, более 3% - студенты.

Самыми распространенными схемами хищения, которые используют преступники, это «звонок из банка» (около 1500 фактов) и «покупка и продажа товаров в Интернете» (более 1000 случаев).

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**

Псевдобанкиры часто звонят жителям региона с подменных номеров, которые маскируются под официальные номера банков. Далее злоумышленники убеждают своих жертв назвать им реквизиты банковских карт, сувс-код, а также смс-пароль. При помощи этих данных они подключаются к мобильному банку потерпевших и похищают все сбережения, а также оформляют от их имени крупные кредиты, после чего перечисляют заемные средства на подконтрольные счета. Кроме того, «банковские мошенничества» совершаются с применением так называемых программ удаленного доступа, с помощью которых киберпреступники получают полный доступ ко всем счетам своих жертв, а также к их личным данным.



ПОЛИЦИЯ КУЗБАССА РЕКОМЕНДУЕТ

**НЕ ДАЙ СЕБЯ
ОБМАНУТЬ!**

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



«Родственник в беде»

ПРИЗНАКИ

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

ЗАПОМНИТЕ:



Задайте собеседнику **вопрос**, ответ на который может знать 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 бездействие является **уголовно наказуемым деянием**



42.мвд.рф

По схеме «покупка и продажа товаров в Интернете» злоумышленники ищут потенциальных потерпевших на сайтах бесплатных объявлений. Для хищения денег они используют различные способы – получают реквизиты банковских карт, убеждают перейти по сомнительным ссылкам якобы для проверки товара, скачать программы удаленного доступа и многое другое.

Сотрудники полиции Кузбасса настоятельно рекомендуют жителям региона никогда не выполнять денежные операции под диктовку неизвестных, кем бы они ни представлялись, не проходить по подозрительным ссылкам, не скачивать неизвестные программы, не называть никому реквизиты своей карты и смс-пароли. Все это может привести к несанкционированному списанию денежных средств с ваших счетов.