По данным ИЦ МВД Республики Саха (Якутия) за 12 месяцев 2020 года зарегистрировано 2287 преступлений, совершенных с использованием информационно-телекоммуникационных технологий (2019 - 1583). Ущерб, причинённый населению республики такими преступлениями составил более 180 млн. рублей. За 3 месяца с начала т.г. зарегистрировано уже 778 таких преступлений (2019 - 472), рост - 64,8 %!

**Почему важно это знать?**

Мобильные и интернет мошенничества в подавляющем большинстве случаев совершаются гражданами, находящимися за пределами территории республики и даже страны. **Преступления, совершенные неустановленными лицами из других регионов**, использующими информационно-телекоммуникационные технологии – **остаются НЕ раскрытыми! Деньги Вам, скорее всего, не вернут!**

**Кто становиться жертвами этих преступлений?**

Является большим заблуждением считать, что на уловки мошенников попадаются только пенсионеры, молодёжь и «недалёкие» граждане. Жертвами, как правило, становятся **работающие граждане трудоспособного возраста от 25 до 55 лет (42,5 %), имеющие постоянный источник дохода**! На пожилых граждан и молодёжь приходится всего 13-14 %.

Жертвами названных преступлений часто становятся граждане активно приобретающие товары и услуги посредством сети Интернет.

**Можно ли распознать мошенника по голосу?**

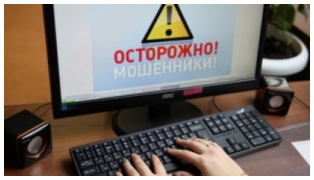
Вы никогда не распознаете мошенника по голосу! Он всегда в разговоре с вами будет вести себя очень непосредственно, квалифицированно, грамотно и предельно корректно, внушая Вам доверие!

**Какие виды мошенничества Вам угрожают?**

По данным полиции в настоящее время на территории республики преобладают 3 наиболее распространённых способа дистанционных хищений:

- мошенники совершают хищения посредством использования подложных объявлений на интернет-площадках;
- мошенники представляются работниками банковских организаций, полиции или других органов или организаций;
- создание злоумышленниками ложных интернет сайтов (близнецов), похожих на сайты известных банков, интернет-магазинов, которые пользуются у потребителей доверием, через которые происходит хищение реквизитов платёжных карт;
- распространение злоумышленниками в сети «Интернет» и социальных сетях предложений заработать на процентах на так называемых «биржах», «инвестиционных компаниях», получить быстрый заработок.
- поддельные биржевые площадки для инвестирования.

**Но это не означает, что нет и не будет других видов. Мошенники ежедневно изобретают новые способы, играя на слабостях людей, а именно на здоровье, беспокойстве за близких, страхе потерять свои деньги, желании купить подешевле, заманчивых и интересных предложениях, денежной выгоде, потребность в заработке, информации для улучшения своей жизни и даже на желании поймать и наказать мошенника!**




**Как совершается интернет-мошенничество?**

Мошенники совершают хищения посредством использования подложных объявлений о купле-продаже или аренде различного имущества на интернет-площадках Авито, Дром, Юла и т.д., причём это могут быть объявления, как о продаже, так и о покупке имущества, в ходе общения под любыми, в т.ч. «объективными», предлогами вам предлагают сообщить данные вашей банковской карты или перечислить аванс за бронирование, в качестве залога и т.д.

Продавец по объявлению может попросить аванс за приобретаемую по объявлению вещь, либо реквизиты вашей карты для перечисления аванса или залога вам, после чего перестанет выходить на связь.

Поэтому следует знать, что приобретение товаров, в т.ч. авиабилетов, либо услуг посредством сети Интернет, не важно в интернет-магазине или с рук у граждан – это большой риск!

Интернет-сайт магазина может оказаться поддельным, а в качестве физического лица – как продавца, так и покупателя – может выступить аферист!

Давно известно, что бесплатный или «супер выгодный» сыр бывает только в мышеловке. Любые активно рекламируемые в Интернет предложения произвести выгодное вложение – мошенничество или финансовая пирамида! Мошенники могут выступать и от имени известных биржевых площадок и вносить предложения, очень похожие на достоверные.

**Как не стать жертвой интернет-мошенничества?**

Нельзя перечислять деньги авансом, да и наложный платёж, к сожалению, не гарантирует, что вы получите именно тот товар, на который вы рассчитывали. Следует лично проверять исправность и наличие в предмете покупки обещанных свойств и возможностей и рассчитываться только по факту получения.

Поэтому либо приобретайте товары в простом магазине либо пользуйтесь только проверенными интернет-магазинами и сервисами, у которых в вашем городе есть офисы, т.к. wildberries, Почта России, aliexpress, причём надо точно знать интернет-адреса этих магазинов, чтобы не попасть на поддельный сайт.

Не делайте покупок со своих зарплатных карт, заведите для покупок специальную карту, например с cashback или travel бонусами, и переводите на неё ровно столько денег, сколько необходимо на покупку.

Авиа и железнодорожные билеты приобретайте в авиакассах или исключительно на проверенном сайте авиакомпании (его адрес можно уточнить по телефону в авиакомпании).

Хотите безопасно инвестировать средства – идите в известный банк, заключайте договор инвестиционного счета!

**Как крадут деньги с банковской карты?**

Основными способами (механизмами) хищений денежных средств с банковских карт граждан являются:

- звонки или рассылка сообщений злоумышленниками, которые представляются работниками банка или служащими. Потерпевшие под воздействием обмана сами передают злоумышленникам персональные данные, одноразовые пароли для входа в приложения (например, Сбербанк-онлайн), в результате чего появляется возможность снятия денежных средств с банковской карты потерпевших;

- совершение покупок в торговых организациях, с помощью ранее похищенной или найденной банковской карты.

Очень часто мошенники представляются работниками банковских организаций, полиции или других органов или организаций и якобы выполняют возложенные на них функции.

Так, например, гражданам поступают звонки такого характера, как:

- *«вам звонят со службы безопасности банка, зарегистрирована попытка несанкционированного списания средств с вашей банковской кары»*. Для отмены или блокировки операции вам предлагают продиктовать реквизиты банковской карты или назвать код, поступивший по СМС, либо предлагают совершить какую-то операцию в банкомате;

- *«взломан ваш личный кабинет мобильного оператора и поэтому вы не получаете СМС-уведомления банка об операциях, совершаемых по вашей банковской карте, вам необходимо назвать код снятия переадресации СМС и т.д.*

Злоумышленники делают повторные звонки даже тем клиентам, которые уже ранее пострадали от действий телефонных мошенников.

Так, имеются случаи, когда по просьбе звонившего якобы сотрудника полиции» граждане даже шли в банк «ловить мошенника»! Одна московская блогерша «повелась» на звонок т.н. «сотрудника полиции» с предложением поймать недавно действительно звонившего ей мошенника и в процессе такой липовой спецоперации потеряла более 1 млн. рублей.

Могут быть и давно известные всем сообщения о том, что «ваш близкий задержан полицией или попал в беду» и нужно заплатить сотруднику полиции или врачу, чтобы спасти.

Вам могут сообщить о начислении денег по ошибке и попросят вернуть средства по другим реквизитам. Деньги по ошибке действительно могут поступить от такого же обманутого человека, но вот попросит вернуть их уже мошенник.

Последнее время получили распространение случаи, когда под видом сообщения с портала Госуслуг могут прислать электронное письмо с предложением ввести страховой номер СНИЛС для дальнейшего получения положенных социальных выплат, а также данные банковской карты, на которую должны поступить деньги. Звонки и сообщения могу прийти и с известного всем номера Сбербанка 900.

**Все способы мошенничества не перечислить, их масса и они постоянно меняются!**

**Как не потерять деньги с банковской карты?**

Ваша материальная безопасность - в ваших руках!

Не надо доверять звонящим вам на сотовый неизвестным гражданам, будь то сотрудник банка, полиции, службы судебных приставов и т.д. Нельзя совершать какие-либо действия с банковской картой, в том числе в банкомате по просьбам и предложениям звонящих вам неизвестных лиц, в т.ч. «банковских работников». Не надо ходить на назначенные вам встречи вне официальных кабинетов банка, полиции и т.д. Найдите сами телефон банка, полиции, судебных приставов и т.д., перезвоните туда и выясните имеется ли та проблема, о которой вам сообщили. Только не надо при этом спрашивать номер телефона у самого звонящего вам неизвестного лица.

В соответствии со ст. 210 Гражданского кодекса РФ гражданин несёт бремя содержания своего имущества, а, следовательно, должен обеспечивать сохранность в т.ч. своего имущества, находящегося на банковской карте, и не допускать их разглашения.

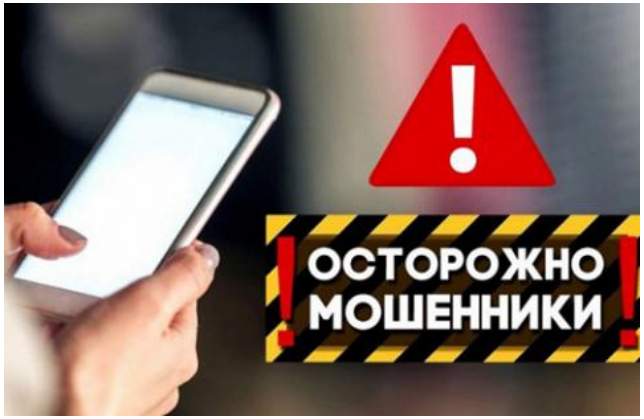
**Ни при каких обстоятельствах НЕЛЬЗЯ сообщать ни кому ПИН-код, CVC-код и срок действия вашей банковской карты, а также коды из СМС оповещения, пароли для входа в мобильный банк и т.д. Это конфиденциальные данные вашей банковской карты!**

Пожалуйста, доведите данную информацию до сведения Ваших родны и близких, защитите их!

Прокуратура Республики Саха (Якутия)
677000, г. Якутск, пр. Ленина, 48,
http://https://epp.genproc.gov.ru/web/proc_14

***Прокуратура Республики Саха (Якутия)***

# *Мобильное и интернет мошенничество. Как распознать и защититься?*




***Граждане, будьте бдительны! Не поддавайтесь на уловки мошенников!***

**Якутск, 2021 год**