МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по КРАСНОЯРСКОМУ КРАЮ
(ГУ МВД России по Красноярскому краю)

ул. Дзержинского, 18, Красноярск, 660017

4/1464 № 28.01.2022

О мерах по предупреждению преступлений, совершенных с использованием информационных технологий

Министру образования и науки
Красноярского края

С.И. Маковской

Уважаемая Светлана Ивановна!

В целях предупреждения и противодействия преступным посягательствам на денежные средства граждан, Главным следственным управлением ГУ МВД России по Красноярскому краю проведен анализ обстоятельств, способствующих совершению хищений денежных средств с использованием информационно-телекоммуникационных технологий[1].

Криминогенная обстановка на территории Красноярского края свидетельствует о незначительном снижении в 2021 году количества зарегистрированных хищений в сфере IT-технологий (с 10168 до 9202). Вместе с тем, продолжается рост регистрации мошенничеств, число которых составило 5520 (+10,7%, или +532 преступлений к АППГ), сумма причиненного материального ущерба гражданам по преступлениям указанного вида составила более 800 000 000 рублей.

По сведениям ОВД края, жертвами мошенников при совершении преступлений, связанных с оформлением кредитов, преимущественно становятся пенсионеры, работники бюджетной сферы, студенты, наемные рабочие.

В ходе расследования уголовных дел установлено, что причинами совершения хищений денежных средств с банковских счетов является не достаточная осведомленность граждан о способах хищений, безопасном использовании банковских счетов и сети Интернет, низкий уровень финансовой грамотности граждан.

Криминалистическими особенностями данного вида преступлений являются: активно развивающаяся сфера применения ИТТ, виктимное поведение потерпевших, применение новых способов совершения

[1] Далее: «ИТТ».

противоправных деяний, тщательно маскируемыми действиями злоумышленников, нахождением их в различных субъектах РФ, использованием для совершения преступлений абонентских номеров и банковских карт, оформленных на третьих лиц, а также осуществлением звонков посредством виртуальных (подменных) номеров (IP-телефония).

Новыми видами мошеннических схем являются:

-фишинг (от англ. Phishing – закидывание удочки) является одной из схем совершения хищений, в результате которой становятся доступны реквизиты банковских счетов граждан и, как следствие, дистанционное управление ими (рассылки в сети Интернет писем с просьбой подтвердить конфиденциальную информацию на сайте организации);

-телефонные звонки о несанкционированном списании денежных средств со счетов. Так, преступник сообщает, что для предотвращения несанкционированного списания денег, гражданину необходимо все свои денежные средства перевести на «безопасный счет», реквизиты которого он сообщает. Фактически потерпевший переводит свои денежные средства на счет преступника;

-«дистанционное оформление кредита». Так, потерпевшему поступают звонки от имени сотрудников службы безопасности банка, которые сообщают, что на потерпевшего оформлен кредит. Для отмены указанной операции необходимо неукоснительно выполнять инструкции преступника, результатом которых в итоге является хищение денежных средств.

При совершении преступлений мошенники используют техники социальной инженерии и нейролингвистического программирования побуждают граждан к оформлению кредитов в одном или нескольких банках. Преступники могут также прибегать к дополнительным методам убеждения, например, сообщают, что в скором времени поступит звонок от сотрудника полиции, который подтвердит, что ранее с потерпевшим действительно разговаривал сотрудник банка и полиция проводит проверку в отношении мошенников. В дальнейшем лица, действующие в сговоре с преступником, осуществляют звонок потерпевшему от имени сотрудников полиции и убеждают выполнить указания лжесотрудника банка. Следует обратить внимание, что при подобной схеме преступления мошенникам доступны технологии «подмены номера», которые позволят видоизменить фактический вид абонентского номера на любой другой, в том числе принадлежащий банковским организациям и органам полиции.

При совершении хищений, связанных с оформлением кредитов, в том числе посредством систем дистанционного банковского обслуживания, потерпевшие либо добровольно предоставляют конфиденциальные данные, позволяющие преступникам похитить со счета денежные средства, либо под воздействием обмана самостоятельно осуществляют операции по переводу преступникам денежных средств, в том числе, предварительно оформив неликвидные кредиты на существенные суммы (от 300 000 до 8 000 000 рублей) в банковских организациях.

Так, в 2021 г. возбуждено уголовное дело по признакам преступления, предусмотренного частью 4 статьи 159 (мошенничество в особо крупном размере) Уголовного кодекса РФ, по факту хищения путем обмана денежных средств в сумме 1 528 000 рублей, принадлежащих работнику бюджетной сферы В.

В ходе предварительного следствия установлено, что в период с 16.08.2021 по 19.08.2021 неустановленные лица, представившись сотрудниками службы безопасности банка и полиции, сообщили потерпевшей не соответствующую действительности информацию об оформлении на ее имя кредитов в банковских организациях, проинструктировав последнюю о том, что для предотвращения негативных последствий она должна продублировать действия «псевдопреступника», получить кредиты и осуществить перевод полученных денежных средств на безопасный счет без штрафных санкций. Потерпевшая, действуя по указанию неустановленных лиц, оформила в двух баках кредиты на общую сумму 1 600 000 рублей. После чего гражданка осуществила перевод денежных средств в общей сумме 1 528 000 рублей на счета абонентских номеров и виртуальных банковских карт, подконтрольных преступникам.

Согласно материалам уголовного дела, ежемесячный доход потерпевшей составляет 53 000 рублей, на момент обращения в банк имелись кредитные обязательства, после оформления указанных кредитов, ежемесячная сумма долговых обязательств составляет более 58 000 рублей.

Кроме того, органами предварительного следствия края расследуется уголовное дело, возбужденное по признакам преступления, предусмотренного частью 4 статьи 159 Уголовного кодекса РФ, по факту хищения путем обмана денежных средств в сумме 1 872 000 рублей, принадлежащих воспитателю детского сада г. Канска Л.

Согласно материалам уголовного дела, Л. 30.11.2021 получила в банковской организации кредитную карту с лимитом 700 000 рублей, обналичила денежные средства в офисе банка и перевела их преступникам. В этот же день Л. оформила кредит на сумму 499 700 рублей. 02.12.2021 вновь обратилась в банк, где получила кредит в размере 200 000 рублей, денежные средства перевела мошенникам. Установлено, что ежемесячный доход потерпевшей составляет около 30 000 рублей, в связи с чем очевидно, что выданные банками кредиты являются неликвидными.

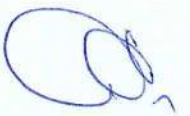
Аналогичным образом в период с 02.12.2021 по 06.12.2021 учитель начальных классов с. Каратузское Красноярского края Т. в двух банковских организациях оформила кредиты на общую сумму 1 512 000 рублей, полученные денежные средства перевела мошенникам.

Согласно материалам другого уголовного дела, потерпевший Л., работающий в должности электромонтера с ежемесячным доходом 50 000 рублей и имеющий кредитные обязательства в двух банках (общая сумма задолженности более 1 000 000 рублей), по указанию мошенников 06.12.2021 получил кредит в размере 950 000 рублей, денежные средства также перевел преступникам.

Таким образом, во всех вышеуказанных случаях сумма обязательных платежей по кредитным обязательствам превысила сумму ежемесячного дохода граждан.

В связи с изложенным, предлагаю довести указанную информацию до сведения подчиненных сотрудников, в целях предотвращения фактов виктимного поведения граждан

Приложение: памятки о профилактике хищений в сфере ИТТ.

Заместитель начальника ГУ -
начальник Главного следственного управления
полковник юстиции  Р.А. Северин

исп.: Изицина А.Н.
тел.: 2919-305

НЕ ДАЙ ОБМАНУТЬ СЕБЯ МОШЕННИКАМ!

1 МОШЕННИКИ ШЛЮТ «ПИСЬМА СЧАСТЬЯ» И ЖДУТ, КОГДА ВЫ ПОПОЛНИТЕ ИХ КОШЕЛЕК СВОИМИ ДЕНЬГАМИ!

НЕ ОТВЕЧАЙТЕ НА ТАКИЕ СМС!!!

- КАРТА ЗАБЛОКИРОВАНА. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ВЫ ВЫИГРАЛИ АВТОМОБИЛЬ! ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- ПОПОЛНЕНИЕ СЧЕТА НА 20 000 РУБЛЕЙ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- НАПОМИНАЕМ ПОГАСИТЬ ЗАДОЛЖЕННОСТЬ ПО КРЕДИТУ. ИНФОРМАЦИЯ ПО ТЕЛ. ХХХХХ
- МАМА, У МЕНЯ ПРОБЛЕМЫ. ПОТОМ ВСЕ ОБЪЯСНЮ. ПЕРЕВЕДИ 300 РУБЛЕЙ НА ТЕЛ. ХХХХХ.

2 У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН

МОШЕННИКИ ПРЕДЛАГАЮТ ПО АКЦИИ УДВОИТЬ ПЕНСИЮ, ПОМОЧЬ ПОПАВШЕМУ В ДТП ВНУКУ, ВНЕ ОЧЕРЕДИ ПРОЙТИ МЕДИЦИНСКОЕ ОБСЛЕДОВАНИЕ.

НЕ ПЕРЕДАВАЙТЕ И НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НЕЗНАКОМЦАМ.
ПРОВЕРЬТЕ ПОСТУПИВШУЮ ИНФОРМАЦИЮ, ПОЗВОНИТЕ РОДСТВЕННИКАМ ИЛИ 02.

3 МОДНЫМ И НАИВНЫМ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯМ ПОСВЯЩАЕТСЯ!

В СОЦИАЛЬНЫХ СЕТЯХ, НА САЙТАХ «АВИТО», «ДРОМ.РУ» ДОВЕРЧИВЫМ ПОКУПАТЕЛЯМ ПРЕДЛАГАЮТ ВНЕСТИ ПРЕДОПЛАТУ ЗА ТОВАР, ОДНАКО В ДАЛЬНЕЙШЕМ СВЯЗЬ С ЛЖЕПРОДАВЦАМИ ПРЕКРАЩАЕТСЯ. У ГРАЖДАН, ПОДАВШИХ ОБЪЯВЛЕНИЯ

МОШЕННИКИ ПОД РАЗЛИЧНЫМИ ПРЕДЛОГАМИ ПЫТАЮТСЯ УЗНАТЬ CVV-код (3 цифры на оборотной стороне карты) ИЛИ ПОДКЛЮЧИТЬ К КАРТЕ УСЛУГУ "МОБИЛЬНЫЙ БАНК".
НЕ В КОЕМ СЛУЧАЕ НЕ СОВЕРШАЙТЕ ЭТИХ ДЕИСТВИЙ!!!

4 РУЧКУ ПОЗОЛОТИ, ВСЮ ПРАВДУ РАССКАЖУ

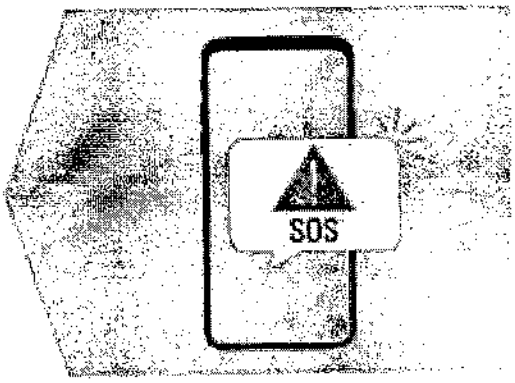
МОШЕННИКИ ПРЕДЛАГАЮТ ЧУДОДЕЙСТВЕННОЕ ИСЦЕЛЕНИЕ ОТ ПОРЧИ ИЛИ СГЛАЗА.
ОДНАКО, ГЛАВНАЯ ИХ ЦЕЛЬ - ЗАВЛАДЕТЬ ВАШИМИ ДЕНЕЖНЫМИ СРЕДСТВАМИ, ЦЕННЫМИ ВЕЩАМИ И СКРЫТЬСЯ. **НЕ ВЕРЬТЕ «ЛЖЕЦЕЛИТЕЛЯМ» И ГАДАЛКАМ!!!**

ГУ МВД России по Красноярскому краю

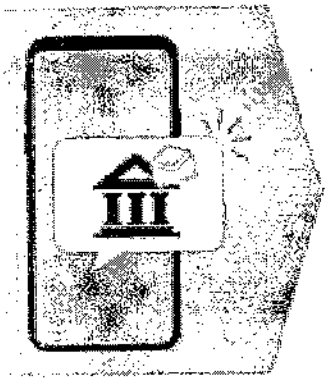
ПРЕДУПРЕЖДАЕТ!

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКОВ НИКОГДА НЕ ЗВОНЯТ КЛИЕНТАМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ ОБ ИМЕЮЩИХСЯ ПРОБЛЕМАХ, СВЯЗАННЫХ С КАРТАМИ!



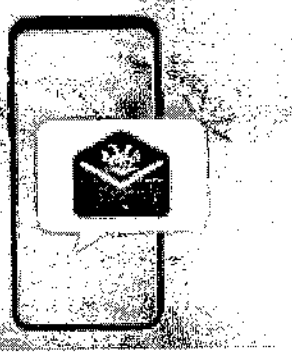
Не следуйте инструкциям звонивших и не отвечайте на задаваемые вопросы, а просто положите трубку!



Проверить информацию можно, позвонив в контактный колл-центр банка по телефону, указанному на задней стороне вашей банковской карты.

Никогда и никому не сообщайте данные своей банковской карты (ПИН-код, код безопасности, пароли и др.)

Знайте, что мошенники уже могут располагать некоторой информацией о ваших персональных данных! Будьте внимательны!



БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

ГУ МВД России по Красноярскому краю

ПРЕДУПРЕЖДАЕТ!

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

«ВАША КАРТА ЗАБЛОКИРОВАНА»

SMS-сообщение о якобы заблокированной банковской карте, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата.

«РОДСТВЕННИК В БЕДЕ»

Требование крупной суммы денег для решения проблемы с якобы попавшим в беду родственником.

«ВЫ ВЫИГРАЛИ»

SMS-сообщение о том, что вы стали победителем и вам положен приз.

«ВИРУСНАЯ АТАКА»

SMS-сообщение, содержащее ссылку на какой-либо интернет-ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте.

«ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ»

Вам якобы положена компенсация за приобретенные ранее некачественные БАДы, либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты.

«ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ»

Просят вернуть деньги за ошибочный перевод средств, дополнительно снимая средства со счета по чеку.

УСЛУГА ЯКОБЫ ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА

ПОМНИТЕ!

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ

Помните! Если вам звонят и тревожным голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники! Никогда не проходите по ссылкам, присланным в SMS сообщении с незнакомых номеров! Никому не сообщайте ПИН-код вашей банковской карты!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКОВ НИКОГДА НЕ ЗВОНЯТ КЛИЕНТАМ ДЛЯ ПРЕДУПРЕЖДЕНИЯ ОБ ИМЕЮЩИХСЯ ПРОБЛЕМАХ, СВЯЗАННЫХ С КАРТАМИ!

Не следуйте инструкциям звонивших и не отвечайте на задаваемые вопросы, а просто положите трубку!

Проверить информацию можно, позвонив в контактный колл-центр банка по телефону, указанному на задней стороне вашей банковской карты

Никогда и никому не сообщайте данные своей банковской карты (ПИН-код, код безопасности, пароли и др.)

Знайте, что мошенники уже могут располагать некоторой информацией о Ваших персональных данных! Будьте внимательны!