МВД России
ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ
ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
по НИЖЕГОРОДСКОЙ ОБЛАСТИ
(ГУ МВД России по Нижегородской области)
ул. М.Горького, 71, Н.Новгород, 603950
тел. (831) 268-51-76, факс 268-63-87

30.07.2019 № 2/3620

на № _____ от _____

Министру транспорта и автомобильных дорог Нижегородской области

В.А. Власову

г. Н. Новгород, ул. Ошарская, д.63, 603115

Уважаемый Вадим Александрович!

Главное управление МВД России по Нижегородской области обращает Ваше внимание на значительное увеличение на территории Нижегородской области количества зарегистрированных хищений денежных средств граждан, совершенных различными способами.

По итогам первого полугодия текущего года на территории региона количество зарегистрированных мошенничеств увеличилось на 13% (до 2412). Также возросло количество краж с банковских счетов граждан. Более 75% данных преступлений совершено бесконтактным способом, то есть с использованием сети Интернет, средств сотовой связи, с банковских карт.

Рост числа указанного вида преступлений обусловлен быстрым развитием информационно-коммуникационных технологий, а также постоянно увеличивающимся количеством лиц, пользующихся различными услугами в сети Интернет, банковскими мобильными приложениями, электронными системами расчетов, в связи с чем прогнозируется дальнейший рост числа преступлений в данной сфере.

В связи с изложенным прошу рассмотреть вопрос об организации размещения на собственных официальных сайтах в сети Интернет, в общественном транспорте публикаций и памяток, направленных на профилактику мошенничеств, в том числе совершаемых с использованием информационных технологий.

Приложение: информация об основных видах мошенничества на 9 л.

С уважением,

И.о. заместителя начальника ГУ-
начальника полиции В.Г. Яремчук

Исп. Боровков В.В.
тел. 8 (831) 2685143

МИНИСТЕРСТВО ТРАНСПОРТА И
АВТОМОБИЛЬНЫХ ДОРОГ
НИЖЕГОРОДСКОЙ ОБЛАСТИ
Вх. №325- от 2019г.

Информация об основных видах мошенничества

В настоящее время наиболее распространенным способом совершения преступлений в данной сфере является хищение с банковских карт граждан, когда злоумышленники по телефону представляются сотрудниками служб безопасности различных банков и под различными предлогами получают от потерпевших номер банковской карты, код CVV (3 цифры на обратной стороне карты), а также пароли, приходившие по SMS, необходимые для проведения финансовых операций. Также злоумышленники могут сообщить потерпевшим о необходимости установления на смартфон, компьютер или планшет различных программ («Anydesk», «Quick support», «Teamviever» и др.), выдавая их, в том числе, за антивирусные, позволяющих мошенникам дистанционно, т.е. удаленным доступом, управлять смартфоном, ноутбуком или планшетом и, как следствие, осуществлять онлайн переводы от имени потерпевших через их личный кабинет.

Обращаю внимание, что в ходе телефонных разговоров мошенники могут сообщить ваши персональные данные: ФИО, дату рождения, паспортные данные, а также даже последние операции по вашим счетам. Кроме того, преступники, используя возможности IP-телефонии, могут осуществлять звонки с абонентских номеров, схожих или идентичных официальным номерам банков, указанным на оборотной стороне карт.

Чтобы не стать жертвой подобных преступлений необходимо помнить, что настоящие сотрудники банков никогда не звонят клиентам и не просят сообщить им какую-либо информацию, касающуюся как их персональных данных, так и банковской карты. Ни при каких обстоятельствах не разглашайте никому, включая сотрудников банков, пароли на проведение операций. Пароль для входа в систему «Банк Онлайн» это ваша личная конфиденциальная информация. Также, не в коем случае не стоит устанавливать по просьбе неизвестных лиц какие-либо приложения (программы).

Иные способы мошенничества совершенные дистанционным способом.

С использованием сети Интернет:

1. Путем получения предоплаты в размере до 100% за товар или услугу с помощью создания «однодневных» интернет-магазинов и сайтов-двойников; с использованием Интернет-площадок по продаже товаров и услуг (сайты «Авито», «Юла» и др.); в социальных сетях «В контакте», «Одноклассники» и т.д.

Прежде чем заказать товар в Интернете почитайте отзывы на разных сайтах о данном интернет-магазине или виртуальном продавце, в случае наличия вы сразу обнаружите отрицательные отзывы, отсутствие отзывов о выбранном вами интернет-магазине говорит о коротком периоде его существования. Внимательно читайте названия Интернет-магазина, тем самым Вы избежите сайтов-клонов. Старайтесь избегать покупки товара по предоплате. Если цена товара гораздо ниже цены в обычных розничных магазинах, так и в других интернет-магазинах, либо на рынке в целом (например, при продаже автомашины по заниженной стоимости), это повод насторожиться.

2. Путем получения информации от лица, разместившего объявление о продаже какого-либо товара, о полных реквизитах его банковской карты

(номер, срок действия, данные держателя, CVC-код), якобы, с целью внесения предоплаты, с последующим хищением с нее денежных средств, используя полученные данные.

Не сообщайте неизвестному какую-либо информацию касающуюся банковской карты - для осуществления перевода требуется только шестнадцатизначный номер карты. Ни при каких обстоятельствах не сообщайте пароли на проведение операций. Пароль для входа в систему «Банк Онлайн» это ваша личная конфиденциальная информация.

3. Путем получения денежных средств от потерпевших при, якобы, внесении ставок на фондовых и иных биржах.

Прежде чем вносить деньги почитайте отзывы на различных сайтах в Интернете, узнайте к юрисдикции какой страны относится деятельность данной организации, а также ознакомьтесь с правилами и условиями ее деятельности.

4. Взлом страниц пользователей в социальных сетях, в основном «Вконтакте» и «Одноклассники», и рассылка сообщений «друзьям» от имени данного пользователя с просьбой одолжить денег, которые нужно перевести на указанные абонентские номера или банковские карты.

Прежде чем осуществить перевод позвоните своему другу, от которого пришло сообщение, и уточните информацию.

С использованием средств сотовой связи путем сообщения гражданам заведомо ложной информации:

1. О нарушении их близкими родственниками действующего законодательства (совершение ДТП, причинение телесных повреждений, хранение наркотиков и т.п.), с целью передачи потерпевшими денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившейся ситуации. При этом мошенники стараются держать «жертву» всегда на связи, с целью исключения каких-либо действий с ее стороны по проверке информации.

Необходимо перезвонить на известные абонентские номера лицу, которым представляется злоумышленник, либо родственникам, с целью выяснения действительности произошедших событий. Попросить звонящего назвать какие-либо данные лица, которым он представляется (Ф.И.О., дата рождения, место жительства, данные родственников, какие-либо факты из жизни и т.д.).

2. О блокировке банковской карты путем рассылки SMS-сообщений и последующего информирования о необходимости дальнейшего введения ряда команд с банкомата.

Прежде чем выполнять какие-либо действия с банковской картой перезвоните в банк и уточните информацию.

3. О возможности получения компенсации за ранее приобретенные некачественные товары или оказанные услуги, для чего необходимо перечислить определенный процент от полагающейся суммы.

Следует знать, что различные компенсации выплачиваются гражданам только при их личном письменном обращении в соответствующие организации. Никакие проценты за выплату компенсаций не уплачиваются.

4. Якобы, из поликлиники или больницы, о том что у Вас или у Ваших родственников обнаружили страшный диагноз и чтобы вылечить болезнь

необходимо перевести деньги за лекарства.

Необходимо помнить, что настоящий врач никогда не будет звонить вам по телефону и сообщать о «страшном диагнозе» или просить перевести деньги за лекарства.

5. С просьбой купить продукты, спиртное, цветы и т.п., доставить их по указанному адресу, а попутно перечислить денежные средства на телефон, с заверением, что деньги вернут по прибытию на адрес заказчика.

Если вы исполняете какое-либо поручение по телефону, доставляете заказы, то не следует переводить деньги на незнакомые телефоны, сначала доставьте товар по назначению и на месте определитесь с заказчиком.

Кроме дистанционных мошенничеств граждане становятся жертвами и контактных мошенничеств, совершенных под видом социальных работников, сотрудников различных организаций (горгаз, горсвет, Пенсионный фонд, медицинские работники и т.д.). Предлогами могут быть: срочный обмен денег, надбавки к пенсии, проверка газового или водяного оборудования, перерасчет квартплаты, премии ветеранам, продажа БАДов, медицинских приборов или других различных товаров по льготным ценам и т.д. Основная цель злоумышленников – узнать, где хранятся денежные средства «жертвы», после чего отвлечь ее внимание и совершить их хищение. Также предлогом может быть гадание, снятие якобы наложенной порчи, исцеление от заболеваний.

Как понять обман:

- об обмене денежных средств или проведении каких-либо реформ заранее будет сообщаться в различных СМИ (телевидение, радио, печатные издания), в отделениях банков, учреждениях социальной политики, пенсионного фонда и т.д.

- узнать, что за организацию представляют пришедшие и, позвонив туда, узнать, есть ли там такие сотрудники и проводится ли обход домов по обозначенному вопросу; попросить предъявить удостоверение;

- уведомить родственников (желательно попросить подъехать);

- позвонить или позвать соседей;

- позвонить закрепленному социальному работнику;

- не стоит покупать у неизвестных никаких лекарственных препаратов, газоанализаторов, счетчиков, фильтров для воды, хозяйственных товаров, медицинских приборов и т.п.

ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

ОСТОРОЖНО МОШЕННИКИ !!!!!

ГРАЖДАНЕ, ПОМНИТЕ, ЧТО О ЛЮБОЙ ДЕНЕЖНОЙ РЕФОРМЕ ВЫ БУДЕТЕ УВЕДОМЛЕНЫ ЗАРАНЕЕ ЧЕРЕЗ СРЕДСТВА МАССОВОЙ ИНФОРМАЦИИ. ДЕНЬГИ НА ДОМУ И В ОБЩЕСТВЕННЫХ МЕСТАХ НЕ ОБМЕНИВАЮТСЯ.

ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

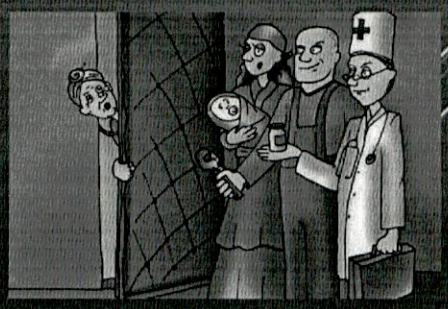
ОСТОРОЖНО МОШЕННИКИ !!!!!

ГРАЖДАНЕ, НЕ ПОКУПАЙТЕ РАЗЛИЧНЫЕ ЛЕКАРСТВЕННЫЕ ПРЕПАРАТЫ И МЕДИЦИНСКИЕ ПРИБОРЫ У ПОСТОРОННИХ ЛИЦ.

ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

ОСТОРОЖНО МОШЕННИКИ !!!!!

ГРАЖДАНЕ, ПОМНИТЕ, ЧТО В НЕКОТОРЫХ СЛУЧАЯХ **ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ** И ИМУЩЕСТВА **ИЗ ЖИЛИЩ** ГРАЖДАН СОВЕРШАЮТСЯ ЛИЦАМИ, КОТОРЫЕ **ПРЕДСТАВЛЯЮТСЯ СОТРУДНИКАМИ РАЗЛИЧНЫХ СЛУЖБ** И ОРГАНИЗАЦИЙ.



ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

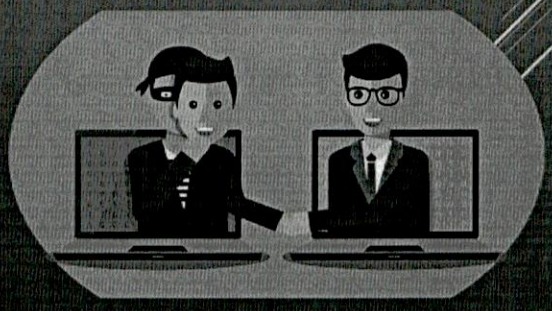
ОСТОРОЖНО МОШЕННИКИ !!!!!

ГРАЖДАНЕ, ПРИ СОВЕРШЕНИИ **ПРОДАЖ В СЕТИ ИНТЕРНЕТ**, НЕ СООБЩАЙТЕ ПОЛНЫЕ РЕКВИЗИТЫ СВОИХ **БАНКОВСКИХ КАРТ** ПРИ ВНЕСЕНИИ **ПРЕДОПЛАТЫ ЗА ТОВАР**.

ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

ОСТОРОЖНО МОШЕННИКИ !!!!!!

ГРАЖДАНЕ, ПРИ СОВЕРШЕНИИ ПОКУПОК В СЕТИ ИНТЕРНЕТ, ОСТЕРЕГАЙТЕСЬ ВНОСИТЬ ПРЕДОПЛАТУ ЗА ТОВАР, А ТАКЖЕ СООБЩАТЬ РЕКВИЗИТЫ СВОИХ БАНКОВСКИХ КАРТ.



ГУ МВД РОССИИ ПО НИЖЕГОРОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ:

ОСТОРОЖНО МОШЕННИКИ !!!!!!

ГРАЖДАНЕ, БУДЬТЕ БДИТЕЛЬНЫ, НИКОГДА НЕ СООБЩАЙТЕ ДАННЫЕ СВОИХ БАНКОВСКИХ КАРТ ПОСТРОННИМ ЛИЦАМ, В ТОМ ЧИСЛЕ ПРЕДСТАВЛЯЮЩИМСЯ СОТРУДНИКАМИ БАНКОВ.

ВНИМАНИЕ! МОШЕННИКИ!

Участились факты мошенничества в отношении пожилых граждан

К Вам пришли работники Пенсионного фонда, социальной, газовой службы или иные лица под различными предлогами пытаются зайти к Вам в дом для оказания услуг или проверки оборудования

- Не спешите пускать их в дом!

- Обязательно посмотрите их удостоверение, позвоните в ту организацию, сотрудниками которой они представились или в полицию по телефону 02!

- Ни в коем случае не показывайте незнакомым места хранения денег и ценностей!

- Будьте бдительны при попытках отвлечь Вас и оставить незнакомца без присмотра в квартире (например, под предлогом принести воды)!

Не оставайтесь равнодушными,
доведите эту информацию до родных и близких!

ВНИМАНИЕ МОШЕННИКИ!

ГУ МВД России по Нижегородской области предупреждает!
В 2019 году жертвами мошенников стали более 2400 жителей области.
Ущерб от их действий составил более 550 миллионов рублей.
Самые распространенные способы мошенничества!

Покупка или продажа товара через интернет-сайт

Если Вы продаете или покупаете какой-либо товар по объявлениям, размещенным на интернет-сайтах, и для перевода денежных средств помимо номера банковской карты Вас просят назвать её ПИН-код, код безопасности (это три последние цифры, расположенные на обратной стороне банквсой карты), а также пароли из телефонных смс-сообщений.

ПОМНИТЕ! ВАМ ЗВОНИТ МОШЕННИК!

НЕ перечисляйте предоплату, не убедившись в надежности продавца.

Мошенничества с банковскими картами

Если Вам пришло SMS-сообщение о том, что Ваша банковская карта заблокирована, необходимо подтвердить операцию по списанию или переводу денежных средтсв.

ПОМНИТЕ! Банки не осуществляют таких рассылок! НЕ звоните на указанные номера телефонов, обратитесь в ближайшее отделение Банка!

ВНИМАНИЕ!

Участились факты мошенничества в отношении пожилых граждан!

Вам позвонили с незнакомого номера и сообщили, что Ваш близкий родственник попал в беду (задержан полицией, совершил дорожно-транспортное происшествие и т.д.), а для того, чтобы помочь, нужна определенная сумма денег. Обязательно проверьте эту информацию, свяжитесь с родными и близкими по ранее известным Вам номерам телефонов!!!

НИ В КОЕМ СЛУЧАЕ НЕ ПЕРЕВОДИТЕ И НЕ ПЕРЕДАВАЙТЕ НЕЗНАКОМЫМ ЛИЦАМ ДЕНЕЖНЫЕ СРЕДСТВА!!!

К Вам пришли работники Пенсионного фонда, социальной, газовой службы и или иные лица под различными предлогами пытаются зайти к Вам в дом для оказания услуг, проверки оборудования и т.д.

-Не спешите пускать их в дом!

-Обязательно посмотрите их удостоверение, позвоните в ту организацию, сотрудниками которой они представились или в полицию по телефону 02 или 102!

- Ни к коем случае не показывайте незнакомым места хранения денег и ценностей!

- Будьте бдительны при попытках отвлечь Вас и оставить незнакомца без присмотра в квартире (например, под предлогом принести воды)!

Не оставайтесь равнодушными, доведите эту информацию до родных и близких!

ВНИМАНИЕ! МОШЕННИКИ!

ГУ МВД по Нижегородской области предупреждает!

Мошенничества на интернет-сайтах

- Под предлогом купли – продажи товара
- Аренда жилья либо помещений
- Трудоустройства

Вы продаете или покупайте какой-либо товар по объявлениям, размещенным на интернет-сайтах, сдаете или хотите арендовать жилье и для перевода денежных средств помимо номера банковской карты Вас просят назвать её ПИН-код, код безопасности (это три последние цифры, расположенные сзади банковской карты), а также пароли из телефонных смс-сообщений.

Помните! ВАМ ЗВОНИТ МОШЕННИК!

НЕ перечисляйте денежные средства, не убедившись в надежности адресата!

Мошенничества с банковскими картами

- Под предлогом разблокировки банковской карты
- Выплат различных компенсаций
- Подтверждения операций по списанию либо переводу денежных средств

Если Вам пришло SMS- сообщение о том, что Ваша банковская карта заблокирована, необходимо подтвердить операцию по списанию или переводу денежных средств

Помните! Банки не осуществляют таких рассылок! Не звоните на указанные в SMS-сообщении номера телефонов, обратитесь лично в ближайшее отделение Банка!

Если Вы стали жертвой мошенников или Вы подозреваете, что в отношении Вас планируются противоправные действия, незамедлительно сообщите об этом в полицию по телефону 02 (с мобильного – 102)