23

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

01.03.21 № 2/1217

на № _____ от _____

Министру образования, науки и молодежной политики Нижегородской области

О.В. Петровой

г. Н. Новгород, ул. Ильинская, д.18, 603950

Уважаемая Ольга Викторовна!

Главное управление МВД России по Нижегородской области обращает Ваше внимание, что по итогам 2020 года количество зарегистрированных краж и мошенничеств, совершенных с использованием информационно телекоммуникационных технологий, увеличилось на 38,3% (с 2421 до 3348) и 73,3 % (с 2641 до 4578) соответственно.

В январе текущего года наблюдается снижение зарегистрированных преступлений данного вида: краж на 22,7% (с 264 до 204), мошенничеств на 8,6% (с 490 до 448). Однако, данные деяния продолжают иметь место и совершаются в массовом характере, причиняя значительный ущерб гражданам.

Значительное число указанных видов преступлений обусловлено 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, образовательных учреждениях публикаций и памяток, направленных на профилактику мошенничеств, в том числе совершаемых с использованием информационных технологий, а также возможность доведения указанной информации в рамках учебного процесса до учащихся и их родителей.

Приложение: информация об основных видах мошенничества на 3 л.

Заместитель начальника полиции В.Г. Яремчук

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

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.

Зачастую потерпевшие, находясь под влиянием мошенников, сами снимают деньги, в том числе оформляют на себя кредиты, и переводят их на абонентские номера или счета, указанные злоумышленниками.

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.

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, или правоохранительных органов, в том числе полиции.

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.

<u>С использованием сети Интернет:</u>

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 или организации где вы

планируете приобрести какие-либо товары, в том числе покупка билетов на все виды транспорта, оплата услуг и кредитов. 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 номер карты, либо привязанный к ней абонентский номер. Ни при каких обстоятельствах не сообщайте пароли на проведение операций. Пароль для входа в систему «Банк Онлайн» это ваша личная конфиденциальная информация.

3. С использованием ссылок в сети «Интернет», перенаправляющих на «фишинговые» (поддельные) сайты, предоставленных мошенниками потерпевшим при оплате товара, размещенного на сайтах «Авито», «Юла» и других, а также при покупке ж/д и авиабилетов, билетов в кинотеатры.

Не переходите по присланным незнакомыми лицами ссылкам и не вводите данные своих банковских карт.

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.

5. 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.

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 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.

3. 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.

4. 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);

- 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.