МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минкультуры России)

125993, ГСП-3, Москва,
Малый Гнездниковский пер., д. 7/6, стр. 1, 2
Телефон: +7 495 629 10 10
E-mail: mail@mkrf.ru

Руководителям
подведомственных Минкультуры России
федеральных государственных музеев,
музеев-заповедников

на № _____ от «____» _____

Уважаемые коллеги!

Направляю для учета в работе информационное письмо Следственного департамента Министерства внутренних дел Российской Федерации о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий.

В целях повышения осведомленности об основных способах совершения мошенничеств, а также мерах их профилактики прошу довести до сотрудников учреждений представленную информацию.

Приложение: на 8 л. в 1 экз.

Директор
Департамента музеев
и внешних связей Е.М.Харламова

Сурин Александр Александрович
+7 495 629-10-10, доб. 1744

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ (МВД России)

Следственный департамент

Мясницкая ул., 3, Москва, 101000

14.12.2023 № 17/2- 42091

на № _____ от _____

О направлении информации

Министерство культуры Российской Федерации

Гнездниковский пер., д. 7/6, стр. 1,2
г. Москва, 125993

Следственным департаментом Министерства внутренних дел Российской Федерации на постоянной основе осуществляется изучение обстоятельств, способствовавших совершению преступлений, в том числе связанных с «дистанционным» хищением.

Наличие возможности использования безналичных форм расчетов, удаленного оформления кредитных договоров, приобретения товаров в онлайн магазинах сети «Интернет» очень удобно, но и позволяет использовать указанные блага в преступных целях. На сегодняшний день преступления, совершенные с использованием информационно-телекоммуникационных технологий, составляют четверть всех зарегистрированных преступлений, а ущерб, причиненный нашим гражданам, исчисляется в миллиардах.

Несмотря на проводимую Министерством внутренних дел Российской Федерации широкомасштабную работу по предупреждению виктимного поведения среди граждан, по-прежнему отмечается недостаточный уровень осведомленности населения об основных способах совершения мошенничеств, а также мерах по их профилактике.

Использование низкого уровня цифровой гигиены населения позволяет злоумышленникам наращивать темпы своей преступной деятельности, лишать граждан последних денежных средств, заключать кредитные договоры, а полученные денежные средства переводить на банковские счета, подконтрольные мошенникам. Кроме того, «играя» на доверчивости граждан, убеждая их, что они участвуют в операциях по пресечению преступной деятельности, заставляют их совершать поджоги государственных учреждений, а также финансово-кредитных организаций.

В этой связи необходимо проведение просветительской работы среди населения с участием учреждений, входящих в состав Министерства.

Особое внимание стоит уделить размещению и доведению профилактической информации среди посетителей театров, кинотеатров, музеев, картинных галерей, выставок, при проведении иных культурных и развлекательных мероприятий.

Вместе с тем стоит отметить, что нередки случаи, когда создаются фишинговые сайты внешне схожие с официальными сайтами театров, музеев, кино, в связи с чем полагаем необходимым на официальных сайтах культурных учреждений разместить предупреждение о возможных действиях со стороны мошенников, осуществлении проверки всех реквизитов сайта перед приобретением билетов.

Также необходимо предусмотреть размещение правил безопасности в билетных терминалах.

В этих целях рекомендуется использовать видео-контент, представленный на официальных сайтах МВД России и Следственного департамента МВД России (https://мвд.рф/вопросы/мошенник, https://мвд.рф/news/rubric/17/).

Также представляется актуальным предусмотреть размещение простых правил «как не стать жертвой мошенников» на бумажных билетах, а при их оформлении в электронном виде включать информацию в рассылку.

Следственным департаментом МВД России с участием потерпевших от преступных действий выпущены видеоматериалы профилактического характера, которые размещены на официальном сайте.

Полагаем возможным разместить ссылки на художественный фильм на сайтах музеев, театров, кино (https://vk.com/video/@digitalarmor).

Кроме того, необходимо рассмотреть вопрос трансляции профилактических материалов наряду с рекламой различных культурных мероприятий на федеральных каналах, баннерах на улицах города и общественном транспорте.

Следственный департамент МВД России готов оказать содействие в предоставлении соответствующих профилактических материалов, а также проведении совместных мероприятий как на районном, так и региональном уровнях.

Контактные телефоны: заместитель начальника Следственного департамента МВД России генерал-майор юстиции Данил Владимирович Филиппов 8(495)667-19-63, 8(495)667-45-04; заместитель начальника управления ведомственного и процессуального контроля Следственного департамента МВД России полковник юстиции Толстобров Алексей Витальевич 8(495)667-10-36, начальник 2 отдела управления процессуального и ведомственного контроля Следственного департамента МВД России полковник юстиции Ильнур Рашитович Якупов 8(495)667-16-61.

Противостоять вызовам и криминальным угрозам возможно только при объединении сил, средств и возможностей!

Приложение: профилактические материалы на 6 л. в 1 экз.

Заместитель начальника Д.В. Филиппов

исп. Ю.Ю. Меньщикова
т. 8 (495) 667 14 34

Информационные материалы об особенностях преступлений, совершенных с использованием ИТ-технологий.

ОСНОВНЫЕ СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

1. Звонки от якобы представителей правоохранительных органов, кредитно-финансовых организаций с сообщением о незаконных действиях с банковскими счетами (совершен перевод денежных средств с принадлежащего жертве счета, пытаются оформить кредит или уже оформили и пытаются обналичить денежные средства, получили доступ к управлению счетом потерпевшего и совершают по нему операцию, срочно необходимо снять все денежные средства и внести их на безопасный счет), также злоумышленники могут сообщать о незаконных операциях с недвижимостью, необходимости оперативного заключения договора купли-продажи.

При совершении таких звонков, потерпевшего называют полными анкетными данными, сообщают сведения о том в каком банке открыт счет. Однако, стоит помнить, что мы все пользуемся различными услугами, получение которых требует от нас регистрации в сети «Интернет», где мы оставляем свои анкетные данные, указываем места жительства, данные банковской карты, что также может быть использовано мошенниками.

В настоящее время граждане стали бдительнее, не поддаются на уловки мошенников и своевременно прерывают такие разговоры.

Указанные обстоятельства заставили злоумышленников при телефонном разговоре сначала говорить на отвлечённые темы, например, о состоянии геополитической обстановки в стране, правах и обязанностях правоохранительных органов и кредитных организаций, тем самым подыскивая подходы к предполагаемой жертве преступления. А уже после, войдя в доверие, получать конфиденциальные сведения для входа в личные кабинеты приложений дистанционного банковского обслуживания или заставлять жертву самостоятельно переводить денежные средства на принадлежащие мошенникам счета.

В настоящее время в условиях неспокойной геополитической обстановки для нарушения общественного порядка злоумышленники совершают звонки потерпевшим, сообщают о том, что специальные службы якобы проводят расследование и выявляют лиц из числа сотрудников банков, органов государственной власти, которыми совершаются преступления. Для пресечения преступной деятельности указанных лиц необходимо содействие. Под четкие указания лиц, совершающих преступления, жертва, считая, что принимает участие в поимке опасных преступников, изготавливает зажигательные смеси, использует их для причинения имущественного ущерба банкам, государству, что создает опасность гибели человека.

2. Звонки от якобы родственников потерпевшего с сообщением, что он попал в беду и ему срочно необходима финансовая поддержка.

Данная преступная схема появилась одной из первых, продолжает быть актуальной. Во время телефонного разговора жертву убеждают, что с ее близким человеком случилось непоправимое и срочно требуются денежные средства для решения проблемы.

Потерпевшему не дают положить телефонную трубку, постоянно держат на контакте, чтобы не дать позвонить близкому человеку и убедиться в его безопасности. Находясь под воздействием обмана, жертвы передают денежные средства злоумышленникам различными способами (перевод на банковские счета, карты, номера телефонов, передача наличных курьеру).

3. Широкое распространение получило незаконное использование персональных данных, личных фото, а также действий потерпевших при посещении различных сайтов в сети «Интернет».

Совершенствование высоких технологий и их применение в повседневной жизни очень удобно. Позволяет быстро получать информацию, приобретать товары. Сами по себе такие возможности и услуги при соблюдении мер предосторожности безопасны.

Однако, граждане, используя сеть «Интернет», не всегда проявляют бдительность. Зачастую не думают, что вводимые ими данные, в том числе персональные, сохраняются на том или и ином сайте, посещают запрещенные ресурсы, переходят по различным ссылкам, предназначенным для собирания информации о лицах. Порой неосмотрительно размещают в сети «Интернет» фото и видео изображения о частной жизни.

Перечисленные обстоятельства позволяют мошенникам использовать собранные данные в противоправных целях. Например, вымогать денежные средства под угрозами распространения сведений о личной жизни. Такие преступления стремительно развиваются.

4. Использование фишинговых сайтов, на которых размещаются сведения об оказании услуг по реализации авиа, ж/д –билетов, бронирование гостиниц, туристические путевки.

В данном случае гражданам, как правило, предлагаются более выгодные цены, условия проживания, туристические поездки по низким ценам. Сайты практически не отличимы от официальных компаний, предлагающих данные услуги. Разница может быть в одной букве или цифре. Однако, необходимо помнить, что невозможно получить качественные услуги ниже рыночной стоимости, перед заключением каких-либо договоров и переводом денежных средств необходимо убедиться в реальности предоставляемых услуг, в том числе ознакомиться с отзывами о данном сайте.

Для хищения денежных средств мошенники также используют предложения по инвестированию денежных средств при проведении различных финансовых операций. Участникам данных проектов предлагается внесение денежных средств, приобретение акций для получения дохода. Предлагаются очень выгодные условия, высокий процент доходности от пользования денежными средствами потерпевшего. После получения денежных средств жертве могут предоставляться сведения об увеличении дохода, различные графики и схемы проведенных с их использованием

финансовых операций, позволяющих сделать вывод о высокой доходности. Однако, данные сведения являются фикцией.

Как правило, о таких сайтах имеется множество отрицательных отзывов в сети «Интернет», которые не изучаются потерпевшими перед внесением денежных средств.

5. Мошенничество в социальных сетях через взлом аккаунта.

Жертва получает сообщение от своего знакомого с просьбой о предоставлении в долг денежных средств, не подозревает, что от его имени действует мошенник. При получении таких сообщений необходимо удостовериться, что с близкими людьми действительно произошли какие-то неприятности, например, позвонив по телефону, не стоит переводить денежные средства неизвестным лицам.

6. Хищение денежных средств под предлогом реализации товара, услуг, объявления о которых размещены на торговых площадках (Авито, Циан, Юля и другие).

Мошенники создают аккаунты на указанных торговых площадках, размещают на них сведения о реализуемых товарах, оказываемых услугах, фактически не намереваясь выполнять обязательства, желая получить денежные средства.

Перед приобретением товаров необходимо внимательно изучить сведения о продавце, дате его регистрации на торговой площадке, имеющиеся отзывы. Мошенники регистрируются незадолго до размещения своих объявлений. Кроме того, не нужно идти выполнять требования продавцов о необходимости полной оплаты товара до его получения, а в случаях когда потерпевшим размещен товар, то требования о необходимости перечислить какую-то сумму, которая в последствии вернется. Данные действия предпринимаются для получения сведений о реквизитах счетов жертвы.

Важно также понимать, что дистанционные мошенники используют разветвленные преступные цепочки. После получения доступа к банковским счетам потерпевших или когда жертва, находясь под воздействием обмана, готова передать мошеннику свои денежные средства, злоумышленникам необходимо в течение нескольких минут принять решение о том, на какие банковские счета перевести похищенные денежные средства, а также как их обналичить. Для этого к участию в преступление привлекаются так называемые «дропы».

«Дропы», фактически, аналогичные промежуточные звенья для вывода похищенных средств. Это физические лица, которые оформляют на себя банковские карты, открывают счета, электронные кошельки. Но делают они это не для личного пользования. Реквизиты передают лицам, совершающим преступления (кураторам).

Полученные от «дропа» реквизиты банковских карт, счетов, электронных кошельков, мошенники называют потерпевшим, которые самостоятельно, действуя под влиянием обмана, переводят на них свои денежные средства.

В дальнейшем «дропы», действуя по указанию мошенников, «обналичивают» денежные средства с использованием различных банкоматов, осуществляют их дальнейший транзит.

Использование «дропов» необходимо мошеннику, чтобы самому «не засветиться» в совершении преступления, избежать наказания, скрыть сам факт киберпреступления и легализовать похищенные денежные средства, используя для их вывода цепочку проведенных операций, создавая сложность в установлении лиц, причастных к совершению преступлений.

Наличие такого инструмента для совершения преступлений приобрело огромные масштабы, из оборота изымается невероятное количество банковских карт, использовавшихся для вывода похищенных денежных средств. Бесконтрольное использование данного инструмента в преступной деятельности привело к функционированию в Российской Федерации «серого» рынка электронных средств платежа, позволяющих выводить огромные суммы денежных средств, похищенных у наших граждан.

Мошенники подробно инструктируют своих «подставных лиц», в том числе о том, какие показания должны быть даны в случае задержания сотрудниками полиции в целях избежание уголовной ответственности. На сегодняшний день мошенниками организованы банки данных «дропов», что позволяет осуществлять их бронирование при совершении преступления, использовать в определенную дату и время конкретного лица.

В настоящее время указанные лица привлекаются к уголовной ответственности, а также к ним имеется возможность предъявления потерпевшей стороной требования о возврате полученных на их счета денежных средств как неосновательного обогащения, поскольку какие-либо гражданско-правовые отношения между ними отсутствуют. При получении предложений об оформлении за денежное вознаграждение банковских карт или открытии счетов на свое имя и передача сведений по управлению счетами или карт другим лицам, необходимо отказаться от таких действий, не становиться соучастником преступления.

В заключении хотелось бы отметить, что обозначенные преступления возможны ввиду несоблюдения правил безопасного поведения, жертва сама предоставляет возможность совершения в отношении нее противоправных действий. В ходе разговора с мошенниками потерпевшие сами сообщают о себе свои сведения, выполняют нелепые требования злоумышленников, такие как снятие со своего счета денежных средств и их внесение на «безопасные счета» мошенников. Сообщают свои конфиденциальные данные, позволяющие мошенникам получить удаленный доступ к управлению банковскими счетами.

Следственный департамент МВД России

Как не стать жертвой мошенника

На сегодняшний день практически нет ни одного гражданина, которому бы не позвонили по телефону и представившись сотрудниками кредитных организаций, правоохранительных органов, потребовали в целях пресечения противоправных действий, связанных с хищением денежных средств с банковских счетов, как можно быстрее перечислить их на так называемые «безопасные» счета, либо срочно скачать какую-либо программу, которая фактически позволяет злоумышленникам удаленно управлять Вашим смартфоном, в том числе совершать операции перевода денежных средств по банковским счетам, используя приложение удаленного банковского обслуживания.

Хищения денежных средств вышеописанным способом составляют четверть от всех совершенных преступлений, их количество и суммы похищенных денежных средств у населения продолжают расти с каждым годом.

Чтобы не стать жертвой мошенника и не лишиться своих денежных средств, необходимо соблюдать элементарные правила поведения. Каждый звонок по телефону, сообщение в мессенджере необходимо воспринимать, как полученные от незнакомого человека, даже если его номер записан в Вашей телефонной книге. Помните, что Вы не видите своего собеседника, а значит не можете быть до конца уверены, что разговариваете именно с тем человеком, которым он представился. **Итак, что же необходимо:**

1. Если вам позвонили и представились сотрудниками банков, правоохранительных органов, то разговор должен быть коротким. При появлении просьб от незнакомца следует насторожиться. Как только у вас возникли сомнения, прекращайте диалог.

Обращайте особое внимание на абонентские номера, с которых приходят сообщения или осуществляются телефонные звонки от лиц, представившихся работниками банка. Часто усыпить бдительность жертвы помогает использование номера, похожего на оригинальный, с которого звонят банковские сотрудники. Помните: отображаемый номер абонента на вашем мобильном устройстве не означает, что именно с него осуществляется звонок, - преступники легко могут осуществить подмену.

2. Ни в коем случае не выполняйте инструкции неизвестных лиц, особенно когда они касаются ваших наличных денежных средств, банковских счетов или карт. Не переводите деньги на якобы безопасные или какие-либо другие счета - вы их потеряете.

3. Необходимо понимать, что ни банки, ни правоохранительные органы не общаются посредством мессенджеров, не просят продиктовать либо сообщить роботу цифры из СМС, трёхзначный код безопасности на обратной стороне карты (CVV2, CVC2), информацию о её сроке действия, остатке денежных средств; перевести деньги на якобы безопасный счёт или по телефону; снять наличные в банкомате; установить приложение для

удалённой техподдержки или управления данными; помочь в расследовании мошенничества, используя ваши счета или наличные денежные средства.

4. Вас должны насторожить извещения о выигрыше в лотерею, в которой вы не участвовали, но для получения денежных средств, необходимо оплатить комиссию.

5. Не переходите по сомнительным ссылкам в сообщениях, а при смене номера мобильного телефона отключайте «Мобильный банк», устанавливайте лимит на списание денежных средств.

6. Получив СМС-сообщение с незнакомого номера о том, что на ваш счёт поступил платёж или списали деньги, немедленно проверьте баланс. Позвоните на горячую линию кредитно-финансовой организации и уточните интересующую информацию.

7. Если Вы получили сообщение от своего знакомого с просьбой помочь их дочке (сыну) победить в конкурсе посредством голосования, для чего необходимо пройти по ссылке, чтобы авторизоваться, не делайте этого. Вы предоставите доступ мошенникам ко всем контактам и возможность отправки от Вашего имени сообщений, например об оказании Вам финансовой помощи.

8. При появлении в сети «Интернет», различных чатах, иных средствах массовой информации объявлений о высоких доходах от вложений денежных средств, не верьте, легких денег не бывает, выгодные условия предлагаются с целью хищения Ваших денежных средств.

9. Не приобретайте услуги по заниженным ценам, такие объявления размещены для хищения денежных средств. Товары и услуги необходимо приобретать на официальных сайтах поставщиков товаров и услуг.

10. Чтобы минимизировать риски, не следует выкладывать персональные данные в Интернет. Необходимо защищать свои компьютеры, планшеты и мобильные телефоны, настроить везде, где только можно, двухфакторную авторизацию, а также всегда использовать надёжные пароли.

Выполняя эти простые правила, вы не станете жертвой аферистов. Подробно расскажите своим родным и знакомым о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, а также о методах защиты от них.

Будьте бдительны! Не дайте себя обмануть!!!!