ГУ МВД России по Нижегородской области

Межмуниципальное управление Министерства внутренних дел Российской Федерации по закрытому административно-территориальному образованию город Саров Нижегородской области (МУ МВД России по ЗАТО г. Саров)

ул. Советская, 1, Саров, 607190
тел. (83130) 6-05-22, 6-06-00

20.09.2023 № 118/11-18138

на № _____ от _____

Главе города Сарова

Сафонову А.А.

проспект Ленина, д. 20 А
г. Саров, 607188

О направлении информации

Уважаемый Алексей Александрович!

По итогам 8 месяцев 2023 года массив преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий увеличился более чем в 2 раза (+103,5 %, с 86 до 175).

141 преступлений или 80,5% зарегистрированных IT- преступлений – это мошенничества и кражи общеуголовной направленности.

Количество зарегистрированных IT-мошенничеств, увеличилось на 87 % (с 69 до 129). Количество краж, совершенных с использованием ИТТ осталось на прежнем уровне - 12.

Указанные преступления составляют 33,1 % от всех зарегистрированных преступлений на территории г. Саров (425). Т.е. каждое третье зарегистрированное преступление – это кражи и мошенничества, совершенные с использованием ИТТ.

Раскрываемость мошенничеств, совершенных с использованием ИТТ, выросла с 7% до 29,9 %.

Сумма ущерба, причиненная гражданам города от онлайн-мошенников, в текущем году составила - 61 млн. 831 тыс. 555 рублей.

Жертвами злоумышленников становятся граждане различного возраста, профессий, занятий и социальных групп.

Первостепенное значение в сдерживании киберпреступности играет осведомленность граждан о новых видах и способах совершения таких деяний.

В настоящее время наиболее распространенными способами совершения дистанционных мошенничеств и краж являются:

1. Путем звонков (как с абонентских номеров обычной сотовой связи, так и IP-телефонии, а также различных мессенджеров: Viber, WhatsApp и др.) гражданам под видом сотрудников различных банков с сообщением о проведении неизвестными лицами, якобы, несанкционированной операции по их счету (списание денег. взятие кредита и т.д.). При этом, зачастую, злоумышленники одновременно представляются

как сотрудниками банков, так и правоохранительных органов (Федеральной службы безопасности, Следственного комитета, Прокуратуры, Министерства внутренних дел) и сообщают, что проводят совместные проверки (разработки) по фактам несанкционированных операций по счетам клиентов и под различными предлогами (иногда – угрозами) вынуждают граждан становиться участниками, якобы, проводимых специальных операций по задержанию преступников в банковской сфере и, в дальнейшем, сообщать реквизиты банковских карт и пароли, либо самостоятельно переводить деньги, в том числе полученные в кредит, на, якобы, «безопастные счета» или абонентские номера или передать их «курьеру».

Также, в некоторых случаях злоумышленники убеждают установить на смартфон различные программы, якобы, являющиеся антивирусными *(«Anydesk», «Quick support», «Teamviever» и др.).* В действительности – это программы, позволяющие дистанционно управлять смартфоном и проводить онлайн переводы от имени потерпевших через их личный кабинет.

В ходе телефонных разговоров преступники могут сообщать персональные данные: ФИО, дату рождения, паспортные данные, номера счетов и банковских карт, а также информацию по последним операциям. Кроме того, они, используя возможности IP-телефонии, могут осуществлять звонки с абонентских номеров, схожих или идентичных официальным номерам банков, указанным на оборотных сторонах карт, а также номерам правоохранительных органов.

Меры профилактики: При возникновении подобной ситуации следует незамедлительно прекратить какое-либо общение со звонящими. 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 любой информации о счетах и картах. В случае возникновения каких-либо вопросов, сотрудники банков просят граждан подойти в ближайшее отделение (офис). Ни при каких обстоятельствах нельзя сообщать никому, включая сотрудников банков, пароли на проведение операций, а также пароль для входа в систему «Банк Онлайн». Также, не в коем случае не устанавливать по просьбе неизвестных лиц какие-либо приложения (программы).

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

Меры профилактики: Прежде чем заказать товар в Интернете необходимо ознакомится с отзывами на разных сайтах о данном интернет-магазине или виртуальном продавце. В случае наличия, можно сразу обнаружить отрицательные отзывы, а отсутствие отзывов о выбранном интернет-магазине говорит о коротком периоде его существования. Свести к минимуму покупки товара по предоплате. Не торопиться с переводом денег (к чему под различными предлогами постоянно подталкивает продавец). Если цена товара гораздо ниже цены как 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.

3. 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 за

товар, с последующим хищением с нее денежных средств, используя полученные данные.

Меры профилактики: Нельзя сообщать неизвестным какую-либо информацию, касающуюся банковской карты, так как для осуществления перевода требуется только номер карты или подключенный к ней номер телефона. Ни при каких обстоятельствах не сообщать пароли, необходимые для проведения операций. Пароль для входа в систему «Банк Онлайн» - это исключительно личная конфиденциальная информация.

4. С использованием ссылок в сети «Интернет», перенаправляющих на «фишинговые» (поддельные) сайты, предоставленных злоумышленниками потерпевшим при оплате товара, размещенного с целью продажи на сайтах «Авито», а также при покупке железнодорожных и авиабилетов, билетов в кинотеатры.

Меры профилактики: Не рекомендуется переходить по присланным незнакомыми лицами ссылкам с дальнейшем вводом данных своих банковских карт.

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

Меры профилактики: Прежде чем вносить деньги, необходимо ознакомиться с отзывами на различных сайтах в сети «Интернет», узнать, к юрисдикции какой страны относится деятельность данной организации, а также ознакомиться с правилами и условиями ее деятельности.

6. Взлом страниц пользователей в социальных сетях, в основном «ВКонтакте» и «Одноклассники», а также аккаунтов в мессенджере «Telegram», и рассылка сообщений «друзьям» от имени данного пользователя с просьбой о предоставлении в долг денежных средств, которые нужно перевести на указанные абонентские номера, счета или банковские карты.

Меры профилактики: Прежде чем осуществить перевод, необходимо позвонить лицу, от имени которого пришло такое сообщение, и уточнить информацию.

7. Хищения денежных средств при заказе товаров на популярных маркетплейсах («Ozon», «Wildberries» и др.). Злоумышленники копируют страницу реального продавца, но выставляют цену ниже рыночной. Спустя некоторое время после того, как клиент оформил и оплатил покупку, его оповещают об отмене заказа и возвращают средства. Далее, с клиентом связывается продавец и предлагает перенести общение в мессенджеры «WhatsApp», «Telegram» или «Viber». При переписке мошенник сообщает, что товар на складе закончился и предлагает воспользоваться сторонним магазином, на который предоставляет ссылку. После перехода по данной ссылке и оплаты покупки на сторонних сайтах, жертва теряет деньги и не получает купленный товар.

Меры профилактики: При общении в мессенджерах, не рекомендуется переходить по присланным незнакомыми лицами ссылкам с дальнейшим вводом данных своих банковских карт.

8. Путем звонков на домашние телефоны пожилым гражданам с сообщением заведомо ложной информации 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 («курьеров»), 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.

Меры профилактики: Необходимо перезвонить на известные абонентские номера лицу, которым представляется злоумышленник, либо родственникам, с целью выяснения действительности произошедших событий или 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.).

На основании п.4 ч.1 ст.12 и п.12 ч.1 ст.13 Федерального закона «О полиции» от 07 февраля 2011 года № 3-ФЗ, прошу Вас данную информацию разместить на информационных стендах и досках Вашего учреждения.

Ответ о проведенных мероприятиях прошу предоставить в адрес межмуниципального управления МВД России по ЗАТО г. Саров в течение трех дней с момента поучения данного письма по основанию предусмотренному ч.4 ст.13 ФЗ «О полиции» от 07 февраля 2011 года № 3-ФЗ.

С уважением,
Начальник А.А. Чернышов

Исп. и печ.: Олейник Е.В.
тел.: 8(83130)60534