ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ
Прокуратура Республики Саха (Якутия)
Саха Өрөспүүбүлүкэтин прокуратурата
Прокуратура г. Якутска
Дьокуускай куоратын прокуратурата
ул. Халтурина, д. 4/1, г. Якутск,
Республика Саха (Якутия), 677000,
тел./факс: (4112) 22-71-35,
e-mail: iaku@14.mailop.ru

405917 968303

07.06.2024 №Исорг-20980035-5087-24/-20980035

На № _____ от _____

Главе городского округа
«город Якутск»

Григорьеву Е.Н.

pressykt@mail.ru

Главе городского округа
«посёлок Жатай»

Исаевой Е.Н.

gojatay@mail.ru

Главному редактору
«Жатайский вестник»

Соколовой О.А.

radkat@rambler.ru

Направляю Вам для размещения на сайте органа местного самоуправления и в сервис быстрого обмена данными Telegram, в газете «Жатайский вестник» следующие статьи.

1. «Распространенные способы дистанционного хищения денежных средств».

На территории г. Якутска наблюдается рост преступлений совершённых с использованием информационно-телекоммуникационных технологий, обусловленный развитием технических возможностей мошенников в области телекоммуникации и информационных технологий, сопровождающийся постоянным внедрением новых способов их совершения и сокрытия.

Наиболее опасными в настоящее время являются так называемые «дистанционные мошенничества» — это хищения, связанные с неправомерным списанием денежных средств с банковских карт граждан, мошенничества, связанные с использованием мобильных средств связи и сети «Интернет».

Наиболее распространенными являются следующие способы дистанционного хищения денежных средств:

- Мошенники представляются жертве сотрудником банка, сообщают, что по его банковскому счету совершаются подозрительные операции и необходимо имеющиеся на банковском счете денежные средства перевести на так называемый «безопасный счет»;

- Путем публикации мошенником объявления о продаже товаров в сайтах объявлений и сервисах по продаже, таких как «Авито», «Озон», «Юла» и т.п. В результате отправки покупателем денежных средств мошенник не направляет в адрес «приобретенный товар»;

- Мошенники могут использовать замаскированные сайты-двойники Интернет-магазинов, посредством которых преступники получают данные банковской карты потерпевшего, доступ к его счету, с которого должны

списываться денежные средства за товар. Главная цель мошенников – получение у потерпевшего номера пин-кода и номера CVV-кодов банковских карт;

- Мошенники звонят жертвам и представляются сотрудником правоохранительных органов, сообщают, к примеру, о том, что их родственник стал виновником дорожно-транспортного происшествия, либо о том, что в отношении них возбуждено уголовное дело, и в целях недопущения в отношении него уголовного преследования следует перечислить денежные средства на определенный счет;

- Телефонные мошенничества, в ходе которых потерпевшему сообщается о выигрыше в лотерее, предлагается перевести денежные средства за пересылку товара, оплатить проценты и т.д.;

- На сотовый телефон или на электронную почту от мошенников приходят сообщения о том, что необходимо перейти по определенной ссылке, либо установить программу, приложение под предлогом защиты от посягательств на денежные средства и прочее. При переходе по ссылке, установке программы, приложения, на телефон или компьютер скачивается «вирус» и происходит списание денежных средств со счета;

- Мошенники по телефону предлагают перечислить денежные средства в инвестиционные компании и получать регулярный доход без затрат времени, предлагают также участвовать в биржевых сделках, открыть и пополнить брокерский счет, обещая быстрый и высокий доход;

- Злоумышленники взламывают персональные аккаунты в социальных сетях или мессенджерах, выкладывают информацию или отправляют сообщения с просьбой перевести денежные средства, объявляют о сборе средств на спасение чьей-либо жизни;

Приведенный перечень не является исчерпывающим, но по смыслу каждого из вышеуказанного способа хищений основной задачей мошенников является установление доверительного контакта с потерпевшим, а потом уже создание условий, при которых денежные средства потерпевшего незаконным путем переходят в распоряжение преступников.

Анализ уголовных дел показал, что в основном преступления в сфере информационно-телекоммуникационных технологий совершаются в рабочее время, а именно после обеда (15 часов до 18 часов по местному времени), поскольку в этот промежуток времени потерпевшие погружены в иные задачи, не всегда способны сконцентрироваться на деталях разговора и хотят быстрее разобраться с отвлекающими факторами. Кроме того, злоумышленники таким образом имитируют реальные call-центы. Как правило, злоумышленники стараются подобрать самый неудобный для клиента момент, помимо рабочих дней, это вечер пятницы, праздничные и отпускные дни.

2. «Профилактика мошенничества в сфере информационно-телекоммуникационных сетей».

В последнее время на территории г. Якутска участились случаи совершения преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий.

Распространены преступления в указанной сфере, связанные с хищением денежных средств граждан.

Одно из наиболее часто встречающихся подобных преступлений – хищение денежных средств со счетов граждан с использованием реквизитов банковских карт. Злоумышленники, как правило, получают такие реквизиты в телефонном разговоре.

Для того, чтобы не стать жертвой мошенников необходимо следовать определенным правилам.

Если получен звонок или сообщение в социальной сети с просьбой о срочной денежной помощи для знакомого или родственника, не стоит принимать решение сразу. Необходимо проверить полученную информацию, связавшись со своими родными и знакомыми.

Сотрудники банка по телефону никогда не запрашивают реквизиты карты – ее номер, срок действия, трехзначный код на обороте. Если сотрудник банка по телефону просит совершить какие-либо операции с картой – это признак мошенничества. Не следует сообщать кому-либо код подтверждения операции из СМС. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека.

Сотрудники банка также не предлагают·

- установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, для удаления вирусов с мобильного устройства);

- перевести денежные средства на «защищенный счет»;

- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.

При сомнительных звонках необходимо положить трубку (прервать телефонное соединение) и перезвонить в call-центр соответствующего банка (номер телефона всегда указан на оборотной стороне карты).

Хищение денежных средств может быть совершено также при совершении онлайн-покупок. При совершении онлайн-продажи товара для получения денег от покупателя достаточно сообщить только номер банковской карты. Если вас просят указать другие реквизиты (например, CVV-код) – это признак мошенничества. Никогда и никому не сообщайте трёхзначный код на обратной стороне Вашей банковской карты (CVV), это ключ к Вашим деньгам.

Имеют место случаи мошенничества с использованием социальных сетей. Например, злоумышленник, обнаружив сохраненный логин и пароль от страницы гражданина в социальной сети, может без разрешения зайти на эту страницу, поменять логин, пароль и от имени гражданина осуществить рассылку друзьям (знакомым) последнего писем с просьбой об одолжении денежных средств. Лицу, получившему такое письмо, следует связаться с гражданином, от имени которого

направлена просьба об одолжении денежных средств, и удостовериться в подлинности письма.

Кроме того, правоохранительными органами зафиксированы факты хищения денежных средств, совершенные с использованием мобильных приложений банков, установленных на телефонах, которые были утеряны их владельцами.

Во избежание подобных случаев целесообразно устанавливать пароль на вход в мобильное приложение. В случае потери либо хищения мобильного телефона с установленным мобильным приложением, вход в которое не защищен паролем, незамедлительно свяжитесь с банком для блокирования операций с банковским счетом.

Разъясняем, что при совершении в отношении вас любых мошеннических действий вам необходимо незамедлительно обратиться в правоохранительные органы, следует максимально подробно рассказать о всех обстоятельствах события. Также следует принять меры к блокировке банковской карты.

Заместитель прокурора г. Якутска

советник юстиции А.В. Валиулов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 00D4AD0464B393D8C58E724DE11AFB75F7
Владелец **Валиулов Алексей Викторович**
Действителен с 05.03.2024 по 29.05.2025

З.В. Местникова