МВД России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ САХА (ЯКУТИЯ)
(МВД по Республике Саха (Якутия))

ул. Дзержинского, 10, Якутск, 677000
тел./факс (4112) 454-896, 454-971
21.12.2023 4/4423
№
на № от

Руководителям министерств и ведомств
Республики Саха (Якутия)
(по списку)

Предотвращение и профилактика киберпреступлений является приоритетным направлением деятельности органов внутренних дел.

Развитие современных технологий с возможностью доступа к различным электронным сервисам, в том числе дистанционного банковского обслуживания, для большинства числа населения является неотъемлемой частью в использовании в повседневной жизни. На фоне этого появляются различные способы и схемы мошенничеств по завладению денежными средствами граждан.

В этой связи, в целях профилактики упреждающего характера среди населения республики Управление уголовного розыска МВД по Республике Саха (Якутия) направляет в Ваш адрес информацию по линии противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, по итогам 11-ти месяцев 2023 года, для использования в служебной деятельности и доведения до подведомственных организаций.

Приложение: информация на 3 л., в 1 экз.

С уважением,

Заместитель министра –
начальник полиции В.М. Арбузов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 654C9A46D8D40E3896A4C6C36BEDE821
Владелец **Арбузов Владимир Михайлович**
Действителен с 13.01.2023 по 07.04.2024

исп.: УУР Николаева О.Г.
☎ 45-48-96

Информация
по линии противодействия преступлениям, совершенным
с использованием информационно-телекоммуникационных технологий
по итогам 11 месяцев 2023 года

По итогам 11 месяцев 2023 года на территории республики рост дистанционных мошенничеств на +43,7%.

На основе анализа преступлений следует отметить, что наиболее подверженными дистанционным хищениям являются лица, относящиеся к возрастной группе ***от 30 до 49 лет (44,1 %).***

Вместе с тем **в 53,7 %** случаев потерпевшими являются представители женской половины населения республики, остальные 46,3 % относятся к мужской половине населения.

Социальный статус потерпевших характеризуется следующим образом: **работающие по найму – 42 %;** пенсионеры - 20 %; лица без постоянного источника дохода – 14,1 %; государственные и муниципальные служащие – 10,9 %; субъекты предпринимательской деятельности – 4,4 %; социальные группы – 8,6 %.

Анализируя временной период хищения денежных средств с использованием ИТТ в отношении жителей республики, можно выделить следующие промежутки: **с 18 ч. 00 мин. до 23 ч. 00 мин.- 38, 2 %, с 14 ч. 00 мин. до 17 ч. 00 мин.- 29,3 %;** с 10 ч. 00 мин. до 13 ч. 00 мин.- 17,5 %; с 00 ч. 00 мин. до 09 ч. 00 мин. – 15,0 %.

Общий ущерб по итогам 11 месяцев 2023 года от дистанционных хищений (158, 159) составил более **827 миллионов рублей**.

Основными и распространёнными видами и способами совершения дистанционных хищений остаются:

- звонки потерпевшему под видом сотрудника банка, который сообщает о проблемах со счетами и предлагает перевести денежные средства на «резервные счета»;
- звонки потерпевшему под видом сотрудника банка, который сообщает о мошеннических действиях в отношении его счета и для отмены операций предлагает сообщить конфиденциальную информацию потерпевшего;
- потерпевший переводит денежные средства после звонка якобы сотрудником полиции, прокуратуры, ФСБ, который сообщает, что его родственник попал в ДТП, и для разрешения данной ситуации необходимо перевести денежные средства;
- потерпевший переводит денежные средства якобы за покупку криптовалюты на сайтах-двойниках или переводит денежные средства на счета физических лиц;
- мошенничества по объявлениям, размещенным на сайтах сети «Интернет» (авито и др.) о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг;
- мошенничества при помощи социальных сетей под видом просьбы финансовой помощи, сбора денежных средств, получения бонусов, предложения дополнительного заработка через инвестиционные компании либо удаленной (дистанционной) работы;

- взлом аккаунтов в мессенджерах «Ватсап» или «Телеграмм», когда потерпевшим от имени человека, который есть в их телефонной книге, приходит сообщение с просьбой занять денежные средства и номер карты куда их необходимо перевести;

- потерпевший заказывает интимные услуги, найдя объявление в сети Интернет и в качестве предоплаты переводит денежные средства;

- взлом (неправомерный доступ) учетных записей «Госуслуги», либо звонки потерпевшему под видом сотрудника этого сервиса, который сообщает о смене контактных данных.

Мошенники придумывают все новые способы обмана доверчивых абонентов. В последнее время участились случаи звонков или сообщений «от имени руководителя»:

- мошенники выдают себя за директора, главврача, ректора университета и других руководителей. Схемы разные: в одних случаях сразу совершают звонок от имени начальника, в других – подделывают аккаунт руководителя в социальных сетях и предупреждают, что с минуты на минуту позвонит сотрудник полиции или ФСБ и Центробанка по очень важному вопросу.

Вопросы могут быть самые разные.

КАК НЕ ПОПАСТЬСЯ?

Даже если звонок или сообщение поступили от «Руководителя», не стоит им безоговорочно верить. Перезвоните начальнику либо возьмите время «подумать» и отложите решение вопроса до утра – на работе выясните все подробности дела.

Многие обманутые граждане говорят о том, что они слышали о схемах, но продолжают верить мошенникам, и свои деньги, а порой кредитные, отправляют им.

МВД по Республике Саха (Якутия) предупреждает:

- **НЕ РАЗГОВАРИВАЙТЕ** с сотрудником банка (или правоохранительных органов, МФЦ, Гос услуги и др.), если Вам позвонили и представились таковыми. В данном случае прекратите разговор и перезвоните на горячую линию банка (организации) сами;

- **ЗАПОМНИТЕ!** Сотрудники полиции, банков и других государственных структур не звонят гражданам и не спрашивают номера банковских карт. В данном случае прекратите разговор,

перезвоните на горячую линию банка сами и обратитесь в полицию;

- **не сообщайте** никому реквизиты банковской карты ПИН-код, CVV/CVC номера (трехзначный код карты на обороте);

- **не проводите операции** по банковской карте по просьбе третьих лиц (они могут подключить себе услугу «Мобильный банк» или приложения «Сбербанк Онлайн» к Вашей банковской карте и произвести снятия денежных средств);

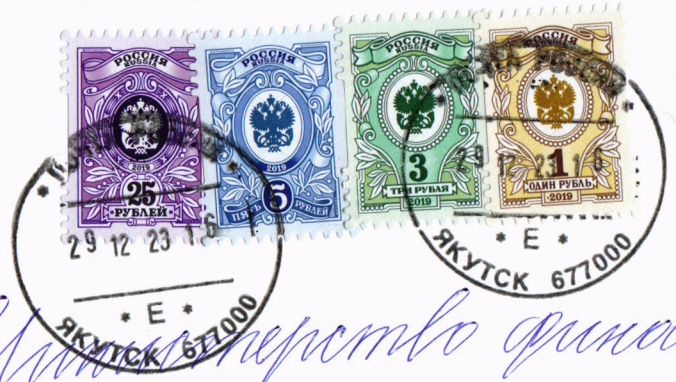
- **не устанавливайте** приложения с неофициальных сайтов особенно на сотовых телефонах с ОС «Android», Вы установите вирус, который получит доступ к Вашим СМС-сообщениям, через которые **спишутся Ваши денежные средства** с банковских карт;

- **не пользуйтесь** сомнительными программами в компьютере и телефоне;

- **не совершайте** покупки в непроверенных интернет-магазинах, страницах/профилях в социальных сетях, если они просят 100% предоплату;

- **проверяйте** на идентичность интернет адреса, электронные почты и профили в социальных сетях с указанными на официальных сайтах информациями, во избежание обмана ресурсом-«двойником».

МВД России
Управление уголовного розыска
МВД по РС (Я)
ул. Дзержинского, 10, г. Якутек, 677000
№ 4/4423



Министерство финансов РС(Я)
ул. Кирова, 12 г. Якутск РС(Я)

677000