ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«РОССИЙСКАЯ АКАДЕМИЯ НАУК»

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«УРАЛЬСКОЕ ОТДЕЛЕНИЕ
РОССИЙСКОЙ АКАДЕМИИ НАУК»
(УрО РАН)**

Первомайская ул., д. 91,
Екатеринбург, 620049
Тел. (343) 374-02-23, факс (343) 374-51-72
E-mail: document@prm.uran.ru

05.12.2023 № 16203-9311/607

На №_____от_____

Руководителям организаций
г. Екатеринбурга
(по списку)

О направлении рекомендаций
по профилактике и предотвращению
мошеннических устремлений

Уважаемые коллеги!

В связи участившимися случаями преступных устремлений к работникам научных учреждений с использованием сотовой связи и сети Интернет, направляем Вам информацию ГУ МВД России по Свердловской области, содержащую данные об известных схемах мошенничества, которые используются преступниками для хищения денежных средств граждан.

Согласно рекомендациям ГУ МВД России по Свердловской области предлагаем рассмотреть данные материалы на коллективном собрании.

Приложение: на 2 л. в 1 экз.

И.о. председателя УрО РАН И.Л. Манжуров

М.И. Кузвесов,
8-919-387-50-41, (343) 374-53-20

Приложение к письму УрО РАН
от 05.12.2023 № 16203-9311/607

На территории Свердловской области участились случаи мошеннических действий с использованием средств сотовой связи и сети Интернет, в отношении работников предприятий и организаций, преследующих цель получить обманным путем доступ к денежным средствам граждан, в т.ч. путем склонения их оформлению кредитов.

С целью исключения подобных случаев, целесообразно довести до работников организации информацию о ставших известными схемах мошенничества.

1. Звонок от сотрудника банка, правоохранительных органов (ФСБ, полиция, прокуратура, следственный комитет) — мошенники представляются сотрудниками правоохранительных органов, используя технологию подмены номеров телефона.

Вместе с тем, сотрудники банков и любых правоохранительных органов НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы денежных средств на какие-либо иные счета.

2. Звонок или текстовое сообщение в мессенджерах (в частности «Телеграмм») – мошенники создают учетные записи в мессенджерах с фотоизображениями и именами реальных руководителей организации (вышестоящей организации), с помощью которых совершают звонки сотрудникам данных организаций, рекомендуя выполнять требования представителей правоохранительных органов и кредитно-финансовых организаций, что в конечном итоге сводится к требованию перевода денежных средств на «безопасные счета».

Вместе с тем, сотрудники банков и любых правоохранительных органов НИКОГДА не спрашивают реквизиты карты, пароли из СМС, персональные данные и не просят совершать переводы денежных средств на какие-либо иные счета.

3. Предложение заработка в инвестиционных проектах (биржи) — мошенники представляются брокерами, предлагая при этом инвестировать денежные средства в различные биржи, после чего, начинают просить оплатить налоги за перевод денег, за комиссии, за страховые премии и т. д.

Вместе с тем, настоящие брокеры не донимают людей звонками и не попросят перевести денежные средства на карты физлиц и другие платежные системы.

4. Заявление о блокировке банковской карты — сообщение о блокировании банковской карты с указанием номера телефона, по которому нужно позвонить. Цель — узнать личный код банковской карты.

5. Объявление о продаже — мошенники продавцы просят перечислить деньги за товар, который впоследствии «жертва» не получает.

6. Объявления о покупке — мошенники, представляющиеся покупатели, стремиться получить информацию о реквизитах банковской карты и (или) смс-кодах якобы для перечисления денег за товар, после чего похищают деньги с банковского счета;

7. Сообщения от друзей — мошенник пользуется чужой страницей в социальной сети в Интернете, и под видом (родственника) просит перечислить ему деньги или сообщить данные банковской карты якобы для перечисления денег под различными предлогами.

8. Звонок о несчастном случае — мошенники звонят «жертве» от лица близкого человека или от представителя власти и выманивают деньги.

9. Получение выигрыша (компенсация за потерянный вклад) — мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. «Жертве» предлагается возможность получить соответствующие денежные средства, заплатив налог или плату якобы «за сохранность денег».

10. Вирусная программа в телефоне — мошенники запускают вирус в телефон, предлагая (в том числе от имени друзей и родственников) пройти по «зараженной ссылке». С помощью вируса мошенники получают доступ к банковской карте, привязанной к телефону.