МВД России

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ ПО РЕСПУБЛИКЕ БУРЯТИЯ
(МВД по Республике Бурятия)

ул. Димитрова, 2а, корп. 2, Улан-Удэ, 670000

12-12-2023 № 10/506

на № _____ от _____

Председателям межведомственных комиссий по профилактике правонарушений городских округов и муниципальных районов Республики Бурятия

Уважаемые руководители!

Направляю в Ваш адрес информационно-справочные материалы об основных видах киберпреступлений, регистрируемых на территории Республики Бурятия, для использования в профилактической деятельности.

Приложение: по тексту, на 2 л. в 1 экз.

Министр О.Ф. Кудинов

исп. Алексеевец А.Г.
тел. (3012)29-52-66

Информационно-справочная информация об основных видах киберпреступлений, регистрируемых на территории Республики Бурятия.

Ежедневно жители Республики становятся жертвами киберпреступников. С начала 2023 года количество потерпевших приблизилось к 6 000, а сумма ущерба превысила 650 млн.рублей.

Самыми популярными IT-преступлениями остаются мошенничества с применением средств связи. Условно их можно разделить на две составляющие.

Первое: «живое общение»

Варианты:

Поступает звонок. Злоумышленник может представляться работником банка, сотрудником службы безопасности банка, представителем правоохранительных структур (МВД, ФСБ, УФССП, Следственного комитета, прокуратуры), представителем оператора сотовой связи, пенсионного фонда, отдела социальной защиты и т.д.

Могут представляться близкими родственниками, либо от его имени.

Примеры разговора:

а) Разговор может заходить о деньгах и их «спасении», переводе денежных средств на «безопасные», «резервные» счета;

б) о поддельных доверенностях на получение денег, о проведении финансовых операций по счетам;

в) о финансировании оппозиции, о подозрении в совершении противоправных деяний, преступлений;

г) об окончании срока действия договора услуг связи;

д) о номере банковской карты;

е) о сообщении кодов, парольно-кодовой информации, поступающих в смс-сообщениях;

ж) просьбы занять деньги;

з) заплатить деньги за «спасение» родственника;

и) установить «полезную» программу, антивирус и др.

Меры защиты: Прервать разговор, перезвонить на номер телефона горячей линии банка, в котором осуществляется обслуживание, позвонить в полицию. Не сообщать никому коды из смс-сообщений. Взять паузу, перепроверить информацию.

Второе: «получение сообщений»

Варианты:

В мессенджеры, групповые чаты, в смс-сообщении, в социальных сетях, на электронные почтовые ящики, поступают сообщения в виде ссылок, смс-сообщений, текстовых объявлений, рекламы.

Примеры сообщения:

а) ссылки где требуется ввод номера банковской карты;
б) об участии в конкурсах, голосовании, где требуется введение номера телефона, кода;
в) об увеличении дохода (об инвестициях), о дополнительных способах заработка с требованием предоплаты, с просьбой банковских реквизитов, кодов доступа;
г) оплата услуг, штрафов, налогов;
д) о необходимости скачивания «полезных» программ;
е) просьбы занять денежные средства;
ж) если аккаунт взломали, могут написать сообщение от руководителя, начальника, родственника, знакомого с просьбой перевода (займа) денежных средств.

Меры защиты: Не участвовать в инвестициях без официального заключения договора, в непроверенных акциях, розыгрышах, конкурсах по полученным ссылкам, рекламам, рекомендациям.

Не сообщать никому коды, не вводить номера банковских карт. Устанавливать приложения только с официальных источников, с большим количеством скачиваний, рейтингом. Использовать актуальные антивирусные программы, официальные сайты для оплаты коммунальных услуг, штрафов, налогов и т. д.

Необходимо взять паузу, перепроверить информацию, перезвонить родственникам, знакомым, в полицию.

СПРАВОЧНО: В странах Прибалтики, Молдавии, Украине ведут криминальную деятельность колл-центры, так называемые специализированные организации, осуществляющие массовые звонки абонентам, что значительно оказывает влияние на рост IT-преступности. В среднем персонал одного колл-центра за неделю совершаются свыше 350 000 звонков, одним сотрудником 3-6 тысяч звонков.

Помните, мошенники не дремлют!
Они каждый день норовят ВАШИ деньги сделать своими!
Сохраняйте бдительность!