**Прокуратура Хоринского района информирует граждан:**

**«Основные виды мошенничества, совершаемых с использованием информационно-коммуникационных технологий. Уголовная ответственность»**

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Согласно Уголовному кодексу Российской Федерации (далее – УК РФ) преступлениями в сфере компьютерной информации, с использованием информационно - коммуникационных технологий, как правило, являются:
 - неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
 - создание, использование и распространение вредоносных компьютерных программ (ст.273 УК РФ);
 - нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и распространение порнографии (ст. 274 УК РФ).

- мошенничество (ст. 159 УК РФ).

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ), а также создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) совершаются только путём действий, в то время как нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – путём как действий, так и бездействием.

Кроме того, распространенный характер носят хищения, связанные с различными способами обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица.

Кроме того, денежные средства могут неправомерно списываться со счетов потерпевших, когда в руки преступников попадают мобильные телефоны потерпевших,  с установленными на них банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

Социальные сети используется также для распространения вирусов. Например, злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Также это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Такая техника остается эффективной, поскольку многие пользователи, не раздумывая кликают по любым вложениям или ссылкам. Особенно это актуально в связи с глобальной цифровизацией общества, которая затрагивает и социально уязвимые слои населения, например, пожилых людей, испытывающих сложности при освоении современной техники, а также страдающих излишней доверчивостью.

В целях пресечения указанных видов преступлений просим всех быть предельно внимательными при осуществлении банковских операций с использованием сети «Интернет» и мобильных телефонов.

По возникшим вопросам Вы можете обратиться в следующие органы:

1. **Прокуратура Хоринского района** +7 (30148) 23-084
2. **МО МВД России «Хоринский»**

+7 (30148) 23-780



***Прокуратура***

***Хоринского района***

***Республики Бурятия***

****

 *«Правовое просвещение населения»*

Февраль 2024 г.