ПРОКУРАТУРА САРАТОВСКОЙ ОБЛАСТИ

ПАМЯТКА

о способах совершения преступлений с использованием информационно-телекоммуникационных технологий и мерах защиты от кибермошенников

(разработана управлением по надзору за уголовно-процессуальной и оперативно-розыскной деятельностью)

г. Саратов, 2025

Современные технологии проникли во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные незаконные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

Подавляющее большинство преступлений совершается с применением методов «социальной инженерии», то есть получение информации с помощью сети Интернет при общении с потенциальными жертвами обмана. Технология основана на использовании психологических слабостей человека и является эффективной.

Например злоумышленник под видом сотрудника банка или иной кредитно-финансовой организации звонит человеку, являющемуся пользователем банковской карты и узнает необходимые реквизиты карты, а также персональные данные человека, ссылаясь на необходимость решения небольшой проблемы в компьютерной системе, предотвращения перевода денежных средств на счета других лиц, необходимости блокировки счета, перевода денежных средств потерпевшего на другие счета, указанные злоумышленником.

Участились случаи взлома личных кабинетов Госсулуг, когда мошенники звонят, представляясь сотрудниками портала Госуслуг, и сообщают о

поступлении на имя потенциальной жертвы письменной информации, для получения которой в почтовом отделении или МФЦ сформирована соответствующая заявка. Затем жертве приходит СМС-сообщение с кодом, который и просит назвать звонящий.

Внимание: работники банков и иных официальных организаций никогда не запрашивают по телефону персональные данные, сведения по счетам, номер карты, сроки ее действия, коды и ПИН-коды от нее, не предлагают перевести деньги на другой счет, либо совершить банковскую операцию.

Каждый звонок от представителя государственного органа посредством сети Интернет через мессенджеры «Ватсап», «Вайбер», «Телеграмм» и другие следует считать подозрительным. Необходимо завершить соединение. Сообщить о звонке на единый номер банка, например «Сбербанк» - 900 и в полицию.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) пострадавших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся ситуации, например освобождения их от уголовной ответственности. Нередко мошенники сами представляются

сотрудниками силовых ведомств.

При поступлении таких звонков, необходимо завершить соединение и позвонить близкому человеку на его личный телефон и в полицию.

Одним из распространенных методов «социальной инженерии» является так называемый «фишинг». Данный метод направлен на получение конфиденциальной информации. Обычно преступник посылает потерпевшему e-mail, подделанный под официальное письмо от банка или платежной системы, требующее проверки определенной информации или совершения определенных действий. Это письмо как правило содержит ссылку на фальшивую веб-страницу, которая является полной копией официального интернет-источника. На фальшивой странице пользователю предлагается ввести необходимую для преступников информацию, начиная от домашнего адреса до пин-кода банковской карты.

Также преступники используют и активно распространяют вредоносные программы. Злоумышленник направляет e-mail, смс-сообщение или сообщение в мессенджере, во вложении которого как указано содержится важное обновление антивируса. Это может быть выгодное предложение о покупке со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе на которую 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.

Внимание: не следует открывать сомнительные электронные письма и сообщения от незнакомых лиц (номеров и сайтов), пользоваться только официальными и проверенными сайтами.

Следует отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые просты в использовании и доступны неограниченному числу пользователей Интернета.

В целях предупреждения преступлений прокуратура Саратовской области призывает жителей региона быть предельно внимательными при осуществлении банковских операций с использованием сети «Интернет» и мобильных устройств.

При любом случае незаконных действий следует обратиться с заявлением в ближайший отдел полиции. В случае отказа в принятии заявления незамедлительно сообщить об этом в районную, городскую прокуратуру или прокуратуру области письменно, путем личного обращения либо по телефону.