Боготольская межрайонная прокуратура Красноярского края информирует!

С начала 2023 года жертвами интернет - преступников стали 9 736 жителей Красноярского края. Причиненный ущерб составил 2 млрд 340 млн. руб.

Большинство преступлений совершается с применением доступа к информации с помощью телекоммуникационных сетей (сотовой связи, ресурсов сети Интернет). Данная преступная технология основана на использовании слабостей человеческого фактора и является достаточно эффективной.

Чтобы не стать жертвой мошенников стоить помнить следующие правила:

- Не сообщайте трёхзначный код на обратной стороне Вашей банковской карты, а также смс-коды от банка — это ключ к деньгам. Помните, сотрудник банка никогда не попросит назвать конфиденциальные данные Вашей банковской карты.
- Если по телефону Вас просят набрать комбинацию цифр в банкомате, прекратите разговор. Никогда не выполняйте действия с банкоматом «под диктовку» другого человека
- Если Вам поступило смс-сообщение с информацией о блокировке Вашей банковской карты, а также указан номер телефона, по которому нужно перезвонить, обратитесь на горячую линию Вашего банка, не перезванивайте по указному в смс-сообщении номеру.
- Если Вам поступил звонок от «сотрудника банка» - который сообщил Вам о блокировки Вашей банковской карты или подозрительных операциях связанных со списанием денежных средств с карты, прекратите разговор и позвоните на горячую линию Вашего банка.
- Если Ваш друг или родственник пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные Вашей карты, чтобы перечислить их Вам, свяжитесь с ним любым другим способом и проверьте, скорее всего, Вам пишет мошенник.
- Если Вам позвонили от имени близкого человека или представителя власти, сообщили о несчастном случае и требуют деньги, прекратите разговор и позвоните близкому. Человек, который выманивает Ваши деньги — мошенник.
- Если по Вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты и смс-код, чтобы перевести деньги, прекратите разговор и ни в коем случае не сообщайте код.

Нередко денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны с установленными на них банковскими сервисами или банковские карты: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа - деньги снимаются в банкоматах.

В последнее время распространение получил так называемый «фишинг» - один из методов направленный на получение конфиденциальной информации, при котором злоумышленник 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, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию - от домашнего адреса до пин-кода банковской карты.

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.

За совершение таких деяний, в зависимости от способа совершения преступлений, предусмотрена уголовная ответственность по статьям 158, 159, 159.3, 159.6 УК РФ.

В случае, если Вы стали жертвой указанных выше мошенников необходимо обратиться в ближайший отдел полиции.

Будьте бдительны и не дайте себя обмануть!