

Прокуратура Киевского района г. Симферополя разъясняет:

Осторожно – мошенники!

В условиях развития цифровой экономики, электронных платежных систем персональных электронных устройств и Интернета стремительно возросло количество совершенных с их использованием преступлений.

Преступники используют различные варианты обмана людей, такие как «Ваш родственник попал в ДТП», «На вас пытаются оформить кредит», «Ваши деньги в опасности», «Вас привлекают к уголовной ответственности», «Скачайте приложение для заработка в интернете» и т.д.

Для предупреждения противоправных действий по дистанционному хищению денежных средств важно запомнить следующее. Сотрудники банка, правоохранительных органов и других государственных учреждений, по телефону или в электронном письме не запрашивают:

- персональные данные граждан (серия и номер паспорта, адрес регистрации, имя и фамилия владельца карты);
- реквизиты, срок действия, ПИН- и CVV-коды банковских карт;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин и пароль для входа в личный кабинет клиента банка.

Сотрудники банка, правоохранительных органов и других государственных учреждений не предлагают:

- установить программы удаленного доступа (или иные сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов);
- перейти по ссылке из СМС-сообщения;
- включить переадресацию на телефоне клиента;
- под их руководством перевести для сохранности денежные средства на «защищённые» или «безопасные» счёта;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

Чтобы не стать жертвой дистанционного мошенничества следует использовать только официальные каналы связи с банками, правоохранительными органами и другими государственными учреждениями.

Важно помнить, что непроверенные приложения, которые могут прислать злоумышленники в личных сообщениях, могут подменять оригинальные приложения, предоставлять доступ к приложениям и мобильному банку. При использовании сотовых телефонов (смартфонов) соблюдайте следующие правила:

- при установке мобильных приложений обращайте внимание на полномочия, которые они запрашивают. Будьте особенно осторожны, если приложение просит права на чтение адресной книги, отправку СМС-сообщений и иных уведомлений, доступ к сети «Интернет»;
- отключите в настройках возможность использования голосового управления при заблокированном экране;

- не переходите по ссылкам из СМС-уведомлений, различных чатов и мессенджеров, не убедившись в их достоверности (перезванивайте людям их приславшим);

- не перечисляйте денежные средства знакомым, родственниками и близким лицам на их просьбы о переводе денежных средств из СМС-уведомлений, различных чатов и мессенджеров, в том числе голосовым сообщениям, не убедившись в их достоверности (перезванивайте людям их приславшим, уточняйте данные о личности); При использовании интернет-сервисов, в том числе для покупки и продажи товаров и оказания услуг (Авито, Юла и т.п.) запомните ряд простых правил:

- используйте средства общения, предоставленные данными сайтами;
- не переходить на «индивидуальное» общение с посторонними лицами с использованием личных номеров телефонов или ссылок на другие сайты;
- не передавайте свои персональные данные, в том числе адрес проживания, контактные телефоны, банковские реквизиты и коды подтверждения банковских операций;
- используйте только порядок и формы оплаты, получения товаров, предусмотренные данными интернет-сервисами.

При оплате товара и услуг в сети «Интернет» (особенно при привязке к регулярным платежам или аккаунтам) требуется всегда учитывать высокую вероятность перехода на поддельный сайт, созданный для компрометации клиентских данных, включая платежные карточные данные. В случае утери или смены номера телефона, привязанного к банковской карте, необходимо:

- связаться с банком для отключения услуги СМС-уведомления;
- заблокировать сим-карту, обратившись к сотовому оператору.

В случае если в отношении совершаются описанные действия, немедленно прекратите разговор и обратитесь в ближайшее отделение полиции с заявлением о совершенном преступлении. Сотрудники полиции обязаны принять Ваше заявление, выдать Вам талон-уведомление, провести процессуальную проверку в порядке ст. 144-145 УПК РФ.

В случае реального хищения денежных средств, уголовное дело может быть возбуждено без проведения проверки, в таком случае Вас признают потерпевшим, допросят в этом статусе. Не верьте словам преступников, если они обещают вернуть денежные средства за совершение определенных действий (порча имущества, поджог зданий, сооружений и т.д.)!