В связи с ростом в Ивановской области количества преступлений с использованием информационных технологий прокуратура Лухского района напоминает о важности защиты персональных данных.

Мошенникам могут быть известны Ваши фамилия, имя и отчество, номера телефонов и банковских карт. Но у них нет кодов доступа к банковским счетам. Чтобы их получить, мошенники могут представиться сотрудниками безопасности Вашего банка, Центробанка, полиции, ФСБ, следственного комитета и т.д.

НИКОГДА и НИКОМУ не разглашайте КОДЫ, ПАРОЛИ, РЕКВЕЗИТЫ ДОКУЕНТОВ, УДОСТОВЕРЯЮЩИХ ЛИЧНОСТЬ, к Вашим банковским счетам. Настоящим сотрудникам банков и правоохранительных органов для исполнения своих должностных обязанностей указанные сведения НЕ ТРЕБУЮТСЯ.

Мошенники могут использовать технологии подмены телефонных номеров и позвонить Вам с номеров МВД, ФСБ, Следственного Комитета, банков («900») и др. НЕ ПОДДАВАЙТЕСЬ обману. Перезвоните сами в дежурную часть полиции.

Сотрудники банковских структур и правоохранительных органов НИКОГДА не будут звонить Вам через мессенджеры, в том числе Viber, WhatsApp и др. Если Вам поступил такой звонок, высвечивается логотип Сбер, ВТБ и пр. – это МОШЕННИКИ.

Не существует никаких БЕЗОПАСНЫХ счетов – не переводите туда свои деньги.

НЕ ИНВЕСТИРУЙТЕ В КАРМАН МОШЕННИКАМ. Не существует ни 100%, ни 200% прибыли от вложенных денег. Биржевой и брокерской деятельностью занимаются лицензированные организации, используются специальные инвестиционные, брокерские счета, иные финансовые инструменты – не переводите деньги на счета физических лиц.

Как не стать жертвой мошенников? Необходимо соблюдать простые правила безопасности:

1. Не разглашать конфиденциальные сведения (коды и пароли). Не хранить банковские карты и пароли к ним вместе, не писать пароли на карте.

2. Не отвечать на незнакомые СМС.

3. Знайте, что при утрате банковской карты ей могут воспользоваться злоумышленники, в том числе без использования PIN-кода (при оплате покупок на сумму менее 3 000 рублей), СМС информирование позволит своевременно среагировать и заблокировать карту.

4. Для обеспечения безопасности пароли к своим аккаунтам в Интернете должны содержать сложные символы и периодически их нужно менять.

5. При совершении покупок в Интернете, Вы можете передать информацию о фамилии, имени, отчестве, адресе жительства (доставки), контактном телефоне, номере банковской карты и т.д. Этих сведений недостаточно, чтобы похитить деньги с банковской карты, т.к. у преступников нет кодов доступа (паролей) к банковскому счету. В этой связи, мошенники всеми возможными способами будут пытаться выманить эту информацию.

6. Мошенники могут использовать технологии подмены телефонных номеров и позвонить с номеров МВД, ФСБ, Следственного Комитета, банков («900») и др. Очень часто используется IP-телефония, в том числе диапазон номеров которых начинается с цифр 8 (495) ... и напоминает нумерацию стационарных телефонов Москвы. Нельзя поддаваться обману.

7. При совершении мошенничеств могут использоваться так называемые «фишинговые» сайты, интернет - страницы, имитирующие торговые площадки, платежные системы и др. ресурсы. Дизайн таких «фейковых» страниц дублирует оформление оригинальных ресурсов. При переходе на такой сайт «двойник» и введении реквизитов карт, денежные средства попадают злоумышленникам.

В любом случае, при любой схеме совершения преступлений основной метод противодействия мошенникам – не совершать необдуманных действий, взять паузу, посоветоваться с родными и близкими, при необходимости обратиться в полицию.

И.о. прокурора Лухского района

советник юстиции В.А. Дубровин

15.04.2024