Уважаемые жители региона!

В последнее время значительно увеличилось количество обращений граждан, ставших жертвами киберпреступлений. Для повышения уровня осведомленности и снижения рисков попасть в ловушку мошенников прокуратура Ставропольского края разъясняет некоторые аспекты киберпреступности и предлагает практические советы по защите ваших прав и законных интересов.

Основные виды киберпреступлений:

Мошенничество с банковскими картами.

Зачастую мошенники получают доступ к вашему счету, используя методы социальной инженерии, предлагая пройти проверку или подтвердить операцию. Важно помнить, что ни один сотрудник банка не вправе требовать от вас номер карты, код из смс или CVC-код.

Фишинг.

Мошенники рассылают письма и сообщения, похожие на уведомления от реальных компаний, сервисов или государственных ведомств. После перехода по указанной ссылке жертва попадает на поддельный сайт, где ее просят ввести личные данные или оплатить несуществующий товар/услугу.

Телефонное мошенничество.

Представляясь службой поддержки банка, представителями правоохранительных органов или близкими людьми, мошенники пытаются выведать у жертвы важную информацию, убедить ее совершить перевод средств или назвать пароль.

Распространение вредоносного ПО.

Попав на компьютер или смартфон, вирусы могу украсть личные данные, блокировать устройство или заставить владельца платить выкуп за восстановление доступа.

Как защититься?

Следование несложным рекомендациям позволит вам обезопасить себя и свое имущество:

- установите надежные пароли и включите двухфакторную авторизацию везде, где это предусмотрено.

- всегда проверяйте источник поступления запросов и уведомлений, особенно если речь идет о предоставлении данных или совершении переводов. - никогда не сообщайте третьим лицам конфиденциальную информацию: полные реквизиты карты, CVV/CVC-код, коды из смс-сообщений.

- устанавливайте антивирусные программы и обновления операционной системы, регулярно проводите сканирование компьютера. - используйте проверенные торговые площадки и банки для оплаты товаров и услуг. Защита собственных средств и сбережений начинается с осознания существующих рисков и правильного поведения в интернете и повседневной жизни. Ваша безопасность в ваших руках!

Что делать, если столкнулись с мошенничеством?

Немедленно обратитесь в ближайший отдел полиции и составьте заявление. Чем быстрее будет зафиксирована информация о произошедшем событии, тем больше

шансов вернуть утраченное имущество. За дополнительной консультацией вы можете обратиться в прокуратуру по месту вашего нахождения.

Уважаемые жители региона! В связи с ростом числа случаев кибермошенничества прокуратура Ставропольского края напоминает о мерах предосторожности, необходимых каждому гражданину для защиты своих финансов и личных данных. За последний период значительно увеличилось количество обращений граждан, пострадавших от действий злоумышленников, применяющих различные методы мошенничества.

Наиболее распространены среди них:

Массовая рассылка фейковых писем. Вам приходит электронное письмо якобы от вашего банка или популярного интернет-ресурса с требованием немедленно изменить ваш пароль или ввести номер вашей карты.

Телефонные мошеннические звонки. Представляются службой безопасности банка или сотрудниками правоохранительных органов, убеждая вас поделиться секретными кодами или перевести средства на «безопасный счет».

Подделанные интернет-сайты. Вы получаете приглашение войти на страницу соцсети или сайта покупки товаров, которая выглядит точно также, как оригинальная страница, но принадлежит мошенникам.

Вредоносные файлы и ссылки.

Получаете файл или ссылку от неизвестного отправителя, содержащий вирус или программу-шпион, позволяющую воровать вашу информацию.

Рекомендации для граждан:

Во избежание рисков, связанных с возможными попытками неправомерного завладения персональными сведениями и финансовыми средствами, настоятельно рекомендуем соблюдать следующие меры предосторожности: - категорически запрещается передавать третьим лицам любые конфиденциальные данные, включая реквизиты банковских карт, пароль, одноразовые коды подтверждения, номер банковской карты и трехзначный код проверки подлинности карты (CVV/CVC). - рекомендуем установить современные средства защиты информационных технологий: использование лицензионных антивирусных программ и своевременная установка обновлений программного обеспечения. - в случае фактического совершения противоправных действий против вашего имущества немедленно предпринимайте следующие шаги: заблокируйте возможность дистанционного управления вашими банковскими ресурсами, зафиксировав происшествие путем обращения в соответствующие подразделения правоохранительных органов, уведомьте банк о факте несанкционированного снятия денежных средств. Обращаем внимание на необходимость соблюдения указанных мер предосторожности для предотвращения случаев мошеннических посягательств.