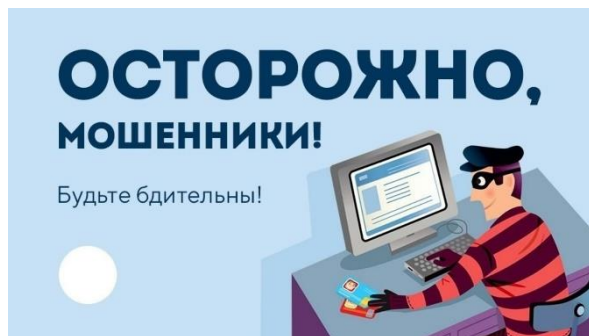




Прокуратура Краснобаковского района информирует:

Ключевую роль в предупреждении преступлений, связанных с хищением денежных средств с использованием сети Интернет, средств мобильной связи, расчетных (пластиковых) карт, играет осведомленность граждан о новых способах и видах их совершения.

В 2024 году от киберпреступлений пострадали 19956 лиц, из них каждый шестой относится к социально уязвимым категориям.



Как не стать жертвой мошенников при продаже личных вещей через сайты объявлений в сети Интернет?

В последнее время распространены случаи мошенничества при поиске покупателей с помощью популярных сайтов объявлений о продаже личных вещей и иных товаров.



Передавать товар стоит только после перевода денежных средств на счет

Так, например, по объявлению приезжает потенциальный «покупатель», осматривает товар и сообщает о переводе денег, называя при этом имя, отчество и первую букву фамилии продавца, тем самым имитируя перевод денежных средств, однако фактически перевод не осуществляет, сообщая об обратном продавцу.

Кроме того, посредством переписки мошенники, действуя под видом покупателя, направляют продавцу ссылку, в которой необходимо ввести реквизиты банковской карты. После проведения указанной процедуры со счета продавца мошенниками списываются денежные средства.

Никогда не переходите по сомнительным ссылкам



Будьте бдительны! Не поддавайтесь на уловки мошенников!

Покупка в интернет-магазине мошенника

Мошенники пользуются все возрастающей популярностью покупок в интернет-магазинах.

Создать "интернет-магазин" и наполнить его фотографиями товаров, которые якобы есть у продавца — дело нескольких минут. После того, как деньги будут перечислены (такие интернет-магазины обязательно требуют предоплату), сотрудники магазина перестают выходить на связь, а потом магазин бесследно исчезает.



- Никогда не совершайте покупки в непроверенных интернет-магазинах, особенно если требуется внесение предоплаты.
- Уточните юридический адрес организации и проверьте через Интернет, существует ли она (например, через сервис 2gis.ru), позвоните, чтобы убедиться в том, что это действительно интернет-магазин.
- Изучите товар по фото, описанию и отзывам покупателей.
- Посмотрите, как вернуть деньги; если такой информации нет, уточните у продавца.

ОБРАТИТЕ ВНИМАНИЕ!

1 От покупки можно отказаться в любое время до получения товара и в течение 7 дней после его получения без объяснения причин.



2 Вы имеете право вернуть товар с нарушенной упаковкой, но в товарном виде и без повреждений.



3 Обратитесь в суд, если продавец не возвращает деньги за возврат товара.



Как обезопасить себя от телефонных вирусов?

СИТУАЦИЯ: на телефон приходит сообщение со следующим текстом: "Вам пришло ММС-сообщение. Для получения перейдите по ссылке...". При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств со счета.

Создание сайтов-двойников - один из способов кражи паролей, номеров кредитных карт, банковских счетов. Внешне такие сайты не отличаются от оригинальных, разница как правило в одной букве адреса. Если не заметить разницы и ввести свои логин и пароль на таком сайте, то эти данные окажутся в руках мошенника.



КАК ОБЕЗОПАСИТЬ СЕБЯ?

- Используйте антивирусные программы.
- Не открывайте с телефона сомнительные ссылки из сообщений.
- Не сканируйте «Qr-коды» из недостоверных источников.
- Не пользуйтесь "банковскими" приложениями, предустановленными на смартфоне, который вы только что купили.

- Обращайте внимание на правильность написания адреса сайта, а также на показатели безопасности сайта, такие как значок закрытого замка в адресной строке браузера и наличие буквы "s" (обозначает "secure"-безопасный), "https://" в начале адреса сайта. Если эти элементы отсутствуют - на такой странице небезопасно вводить данные, особенно реквизиты банковских карт.
- Не скачивайте приложения с неизвестных сайтов, из неофициальных магазинов приложений, по ссылкам, которые содержатся в электронных рассылках, рекламе в социальных сетях.



ПОМНИТЕ!

Перейдя по сомнительной ссылке или установив "безопасное" приложение, Вы открываете доступ к своим персональным и платежным данным.