Прокуратура Грязовецкого района разъясняет:

Некоторые виды дистанционного мошенничества:

«Фишинг»

Еще один вид интернет-мошенничества «фишинг», целью которого является **получение доступа к конфиденциальным данным пользователей — логинам и паролям.** Мошенники при помощи рассылок через различные мессенджеры от лица банка дают потенциальной жертве ссылку на страницу, на которой предлагается вести определенные конфиденциальные данные.

Хищения с карт, подключенных к опции бесконтактных платежей

Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма **не превышает 1 000 рублей.** При этом количество расходных транзакций не ограничено.

Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Ошибочный перевод средств

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». **В действительности деньги не поступают на телефон, а человек переводит свои собственные средства.** Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

Прокуратура Грязовецкого района разъясняет:

Некоторые виды дистанционного мошенничества:

Рассылка писем по электронной почте

Рассылка писем с сообщением о выигранном призе или о блокировке счета. Преступники, как правило, просят победителя перевести определенную сумму для получения крупного выигрыша или внести оплату для разблокировки карты.

Как уберечься от телефонных мошенничеств?

Чтобы не стать жертвой злоумышленников, **необходимо соблюдать простые правила** безопасного поведения и обязательно довести их до сведения родных и близких:

1) не следует отвечать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги;

2) не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;

3) не следует сообщать по телефону кому бы то ни было сведения личного характера.

ВАЖНО! За мошенничество в сфере компьютерной информации предусмотрена уголовная ответственность (ст. 159.6. «Уголовного кодекса РФ»)

ПОМНИТЕ! Своевременное обращение в правоохранительные органы может помочь другим людям не попасться на незаконные уловки телефонных мошенников. Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью.