МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД «ЗОЛОТОЙ ПЕТУШОК» Р.П. СРЕДНЯЯ АХТУБА СРЕДНЕАХТУБИНСКОГО РАЙОНА ВОЛГОГРАДСКОЙ ОБЛАСТИ

404143, Волгоградская область, р.п.Средняя Ахтуба, ул.Октябрьская, 89А
тел.8(844-79) 5-25-20 E-mail: srd_dsad.zolpet@volganet.ru

Памятка по профилактике преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Уважаемые коллеги!

На сегодняшний день информационно-телекоммуникационные технологии затрагивают все сферы жизни человека. Наряду с этим, стремительно возрастает количество преступлений, которые совершаются с использованием данных технологий.

На территории Российской Федерации распространено **дистанционное мошенничество**, к которому относятся:

1. «**Фишинг**» – вид дистанционного мошенничества посредством разговора по телефону или направления электронного письма или смс-сообщения, при котором злоумышленники получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств.
2. «**Фарминг**» – направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг;
3. «**Двойная транзакция**» - «ошибка» при оплате товаров или услуг с предложением повторить операцию, в дальнейшем денежные средства списываются дважды по каждой из проведенных операций;
4. «**Траппинг**» - манипуляция с картридером банкоматов, позволяющая не возвращать карту владельцу или списывать все данные карты для дальнейшего их использования.

Чтобы обезопасить себя и своих близких от различных схем мошенников необходимо запомнить и выполнять следующие рекомендации:

1. **Установить на телефон или компьютер** современное лицензированное **антивирусное программное обеспечение**.
2. Не устанавливать и не сохранять без предварительной **проверки антивирусной программой файлы, полученные** из ненадежных источников.
3. **Не использовать пароли, связанные с персональными данными**.
4. Необходимо убедиться в достоверности информации, полученной в ходе телефонного разговора и интернет-переписки с неизвестными. Мошенники могут представляться сотрудниками правоохранительных органов, представителями операторов сотовой связи и банковских учреждений, знакомыми и даже вашими родственниками. **Следует связаться с теми, от чьего имени действуют незнакомцы и убедиться в правдивости информации**. Не стоит бояться прервать разговор.
5. Ни при каких обстоятельствах **не следует сообщать реквизиты своих банковских счетов и карт (номер карты, срок её действия, секретный код на оборотной стороне карты**). Сотрудники банка никогда не просят сообщить данные вашей карты или пройти к банкомату.
6. **Никогда нельзя переводить денежные средства**, если об этом вас просит ваш знакомый в социальной сети. Возможно, мошенниками был взломан аккаунт, **сначала необходимо связаться с этим человеком** и узнать, действительно ли он просит у вас деньги.
7. **Поставить лимит на сумму списаний или перевода в личном кабинете банка**;
8. В случае возникновения вопросов обращаться в банк, выдавший карту.
9. **Не перезванивать по номерам и не переходить по ссылкам**, которые приходят на e-mail или по SMS.

<u>Будьте бдительны и не поддавайтесь на уловки мошенников</u>!

Способы и методы совершения краж и мошеннических действий постоянно меняются. **В случае малейших подозрений на обман незамедлительно сообщайте об этом в правоохранительные органы по телефону «02» или «112».**