

Профилактическая беседа с сотрудниками МБДОУ Урской детский сад «Росинка» на тему кибермошенничества.

20 ФЕВРАЛЯ 2025г.

     В связи с участившимися случаями кибермошенничества  в нашем детском саду была  организована профилактическая беседа с сотрудниками на тему киберпреступлений. **Ответственный по АТЗ Мельник Марина Павловна**рассказала присутствующим, что такое киберпреступность, посмотрели видеоролик о кибермошенничестве, а также раздала памятки «Как не стать жертвой киберпреступления».

     Киберпреступность является новой и одной из быстроразвивающихся формой транснациональной преступности. Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

**Что такое киберпреступление?**

В настоящее время при характеристике компьютерных преступлений используется целый ряд понятий: "информационное преступление", "киберпреступление", "преступление в сфере компьютерной информации", "преступление в сфере высоких технологий", "виртуальное преступление".

      Согласно действующему законодательству, в содержание понятия **"компьютерная преступность"**включают:

1)**преступления против информационной безопасности**(модификация компьютерной информации, несанкционированный доступ к компьютерной информации, компьютерный саботаж, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

2) **хищения путем использования средств компьютерной техники**;

3) **изготовление и распространение порнографических материалов или предметов порнографического характера, в том числе с изображением несовершеннолетнег**о;

4) **иные преступления, так или иначе связанные с использованием компьютерной техники:** доведение до самоубийства путем систематического унижения личного достоинства через распространение каких-либо сведений в сети Интернет; разглашение врачебной тайны; незаконное собирание либо распространение информации о частной жизни; клевета; оскорбление; распространение ложной информации о товарах и услугах; заведомо ложное сообщение об опасности; шпионаж; умышленное либо по неосторожности разглашение государственной тайны; умышленное разглашение служебной тайны и др.

     Таким образом, к **компьютерным преступлениям** относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

    Киберпреступность принимает самые различные формы, чаще всего – преступлений, связанных с персональными данными. Они могут совершаться при помощи **"фишинга"** (обмана пользователей сети Интернет с целью заставить их сообщить свои персональные данные), **вредоносных программ** (программного обеспечения, устанавливаемого без ведома пользователя и собирающего персональные данные) и **взлома** (незаконного получения удаленного доступа чужому компьютеру). Как правило, подобные методы применяются мошенниками для кражи данных кредитных карт и денежных средств. Кроме того, через Интернет все чаще совершаются преступления, связанные с нарушением авторских прав и прав интеллектуальной собственности, а также распространением материалов с детской порнографией и сценами насилия.

**Как не стать жертвой киберпреступления?**

1. **Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт**, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка "от сотрудника банка" необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк. Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если "сотрудник банка" в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

**ВНИМАНИЕ: помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджер (Vibe, Telegram, WhatsApp).**

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, **обязательно проверяя доменное имя ресурса в адресной строке браузера.**

3. **Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут доступны посторонним лицам**; это же относится к фотографиям и иным видам информации конфиденциального характера.

4. **Следует воздерживаться от онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги**, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт **по просьбе пользователей сети Интернет.**

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам **необходимо использовать сложные пороли, исключающие возможность их подбора.** Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

7. При составлении платежных документов **важно проверять платежные реквизиты получателя денежных средств.**

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории "друзья", с просьбами о предоставлении реквизитов банковских платежных карточек **не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных связей**.

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

10. **Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров**; не переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо **использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу**  не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

12. Следует **ознакомить с перечисленными правилами безопасности своих родственников и знакомых**, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.