Информационная безопасность школьника

Примеры действий мошенников

Приобретение аккаунтов

- Украинские мошенники приобретают аккаунты российских школьников за 7-10 долларов, чтобы распространять призывы к диверсиям и ложные сообщения о терактах.

- Из-за ограничений на создание новых страниц они используют уже существующие профили.

- Родителям необходимо предупредить своих детей об этой опасности, так как подобные действия могут привести к нежелательным последствиям.

Массовые звонки учащимся

- Зарегистрированные массовые попытки мошенничества в отношении учащихся школ.
- Мошенники звонят ученику якобы от представителей администрации школы и сообщают о сбое в МЭШ.
- Злоумышленники сообщают о необходимости срочного восстановления пароля от Электронного журнала (дневника), иначе все данные будут утеряны.
- Далее мошенники выманивают код-пароль из смс и получают доступ к аккаунту ученика для доступа к МЭШ, и/или порталу Госуслуг муниципального образования.

Попытки выманивания средств родителей

- Продолжаются попытки мошенников заполучить средства родителей, воздействуя на детей.
  Преступники представляются сотрудниками «Почты России», «Госуслуг», сотрудниками спецслужб, убеждают детей в необходимости «задекларировать» ценные вещи семьи.
- Используя угрозы и психологическое давление, злоумышленники заставляют выносить и отдавать курьерам деньги, ценные вещи и золотые украшения.
- Основной инструмент преступников – угрозы возбуждения уголовных дел в отношении родителей.
  Естественное желание защитить свою семью может сыграть злую шутку, и предупредить это не просто.

О чем необходимо поговорить со своими детьми?

Объясните ребенку, что мошенники могут притворяться кем угодно.

- *«Не все люди в Интернете и по телефону – те, за кого себя выдают. Кто-то может называть себя учителем, полицейским или даже другом, но на самом деле быть мошенником».*

Объясните, что мошенники могут запугивать.

- *«Иногда обманщики говорят, что если ты им не поможешь, твои родители попадут в беду. Например, могут угрожать, что мама или папа нарушили закон и срочно надо перевести деньги, иначе будет плохо».*

Научите ребенка обращаться ко взрослым в любой тревожной ситуации.

- *«Если тебе что-то кажется странным, страшным или подозрительным – сразу расскажи мне».*

Покажите ребенку, как себя защитить:

- Разберите образец обмана – вместе обсудите, как выглядят фальшивые сообщения и звонки.
- Настройте приватность в соцсетях – минимизация находящейся в открытом доступе информации поможет избежать подготовленных мошеннических схем.
- Установите семейные правила – ребенок не передает никому личные данные, не отправляет фото документов, не сообщает коды из SMS.

Придумайте кодовое слово для вашей семьи

- Мошенник может позвонить с номера телефона вашего близкого и даже подделать его голос с помощью технологии Deep fake. Но защититься от такой сложной технологии довольно легко. В случае, когда кто-то говорит голосом вашего близкого, но вы чувствуете что-то неладное, попросите назвать его кодовое слово. Мошенник, конечно же, не сможет этого сделать.

Новая схема мошенничества - доступ к банковским счетам родителей

Как это происходит:

- Мошенники устанавливают контакт с детьми через игровые чаты, мессенджеры или звонки, маскируясь под службы доставки или других доверенных лиц.
- Злоумышленники пытаются выманить у детей данные для доступа к личному кабинету онлайн-банка родителей (логины, пароли, коды подтверждения).
- Особенность данной схемы — атаки происходят ночью, когда взрослые спят и не могут вовремя отреагировать.

Рекомендации для защиты:

- **Проведите беседу с детьми.**
  Объясните, что нельзя делиться личной информацией, паролями или кодами из SMS/сообщений, даже если их просят "представители спецслужб" или "друзья по игре".
- **Установите родительский контроль.**
  Ограничьте доступ детей к подозрительным сайтам и мессенджерам в ночное время.
- **Используйте двухфакторную аутентификацию.**
  Это усложнит доступ к вашему банковскому аккаунту даже в случае утечки данных.
- **Проверяйте активность в онлайн-банке.**
  Регулярно отслеживайте операции по счету, чтобы вовремя заметить подозрительные действия.
- **Сообщайте о подозрительных случаях.**
  Если ваш ребенок столкнулся с подобной ситуацией, немедленно сообщите в банк и правоохранительные органы.

Важно:

- Мошенники активно используют доверие детей и их неопытность.
- Ночные атаки направлены на то, чтобы родители не успели среагировать вовремя.