Уважаемые учащиеся и родители!

В современном мире кибермошенничество становится все более распространенным. Чтобы защитить себя и своих близких от преступных действий в интернете, важно знать основные правила безопасности и быть бдительными. Эта памятка поможет вам избежать неприятностей и сохранить ваши деньги и личные данные.

Основные виды кибермошенничества, с которыми вы можете столкнуться:

Получение обманным путем вашей личной информации (пароли, номера банковских карт, логины) через поддельные сайты, электронные письма или сообщения в социальных сетях, маскирующиеся под официальные источники (банки, социальные сети, государственные органы).

Мошенничество в социальных сетях: Создание поддельных аккаунтов друзей или родственников для выманивания денег или личной информации. Предложения выиграть ценные призы в конкурсах, требующие предоплату.

Мошенничество при онлайн-покупках: Продажа несуществующих товаров или подделок через интернет-магазины или доски объявлений. Требование предоплаты за товар или услугу.

Взлом аккаунтов: Получение несанкционированного доступа к вашим аккаунтам в социальных сетях, электронной почте, онлайн-играх.

Мошенничество с использованием мобильных приложений: Заражение вашего телефона вредоносным программным обеспечением через скачивание приложений из неофициальных источников.

«Звонки из банка»: Мошенники представляются сотрудниками банка и под предлогом предотвращения "несанкционированных операций" или «компрометации карты» пытаются выманить данные вашей карты или убедить перевести деньги на "безопасный счет".

Правила безопасного поведения в интернете:

1. Будьте бдительны:

- Никогда не переходите по подозрительным ссылкам, особенно в электронных письмах и сообщениях от незнакомцев.
- Внимательно проверяйте адрес сайта в адресной строке браузера.
- Не доверяйте сообщениям, в которых вас торопят принять решение или предлагают слишком выгодные условия.
- Не делитесь личной информацией (пароли, номера банковских карт, PIN-коды) с кем бы то ни было.
- Помните, что сотрудники банков никогда не запрашивают PIN-коды и CVV-коды банковских карт.

2. Защитите свои аккаунты:

- Используйте сложные и уникальные пароли для каждой учетной записи.
- Включите двухфакторную аутентификацию везде, где это возможно.
- Не используйте один и тот же пароль для разных сайтов и сервисов.
- Регулярно меняйте свои пароли.
- Не сообщайте свой пароль никому.

3. Совершайте безопасные онлайн-покупки:

- Покупайте только на проверенных и известных сайтах.
- Проверяйте отзывы о продавце.
- Используйте безопасные способы оплаты, такие как кредитные карты или платежные системы с защитой покупателя.
- Не переводите деньги незнакомым лицам.
- Остерегайтесь слишком низких цен – это может быть признаком мошенничества.

4. Защитите свои устройства:

- Установите антивирусное программное обеспечение и регулярно обновляйте его.
- Скачивайте приложения только из официальных магазинов (App Store, Google Play).
- Не открывайте подозрительные файлы, полученные по электронной почте или в сообщениях.
- Регулярно обновляйте операционную систему и другое программное обеспечение на своих устройствах.

5. Будьте осторожны в социальных сетях:

- Не принимайте запросы в друзья от незнакомых людей.
- Ограничьте доступ к вашей личной информации в профиле.
- Не публикуйте слишком много личной информации, такой как адрес, номер телефона, расписание занятий.
- Сообщайте о подозрительных аккаунтах и сообщениях.

Что делать, если вы стали жертвой кибермошенничества:

1. Немедленно сообщите о случившемся в полицию (ближайший отдел полиции или по телефону 102).
2. Заблокируйте свою банковскую карту, обратившись в банк.
3. Измените пароли от всех своих аккаунтов.
4. Предупредите своих друзей и родственников, чтобы они были бдительны.
5. Сохраните все доказательства мошенничества (электронные письма, сообщения, скриншоты).

Памятка для распространения среди родственников:

1. Поговорите со своими бабушками и дедушками об основных правилах безопасности в интернете. Объясните им, как распознать фишинговые письма и подозрительные звонки.
2. Помогите им установить антивирусное программное обеспечение и научите им пользоваться.
3. Объясните им, что нельзя сообщать свои личные данные по телефону или через интернет.
4. Убедитесь, что они знают, куда обратиться за помощью, если стали жертвой мошенничества.

Помните: ваша бдительность – лучшая защита от кибермошенников!

Разработано Управлением образования Администрации городского округа город Уфа Республики Башкортостан.