Что можно предложить в качестве инструмента противодействия мошенникам? Прежде всего, естественно, здравый смысл.

В первую очередь следует сохранять спокойствие и не поддаваться на провокации. Необходимо как следует проверять все ссылки и сайты, на которые эти ссылки ведут.

Если вы получили подозрительную ссылку от друга, прежде чем на неё перейти, стоит убедиться, что её послал именно ваш друг. В идеале на сайты, требующие ввода личных данных, ходить по ссылкам вообще не стоит — лучше набрать адрес вручную. Разумеется, посещение подобных ресурсов должно осуществляться через надёжные устройства и сети.

Не забывайте использовать и регулярно обновлять антивирусные продукты, особенно если они предоставляют вам и антифишинговые решения. Например, модуль "Антифишинг", встроенный в *Kaspersky Internet Security*, умеет не только сверяться со списком уже известных мошеннических сайтов, но и опознавать потенциально опасные по более чем 200 критериев.

**Краснодарская краевая детская библиотека
им. братьев Игнатовых
ул. Красная, 26/1**

www.ignatovka.ru

Внимание: виртуальные мошенники!

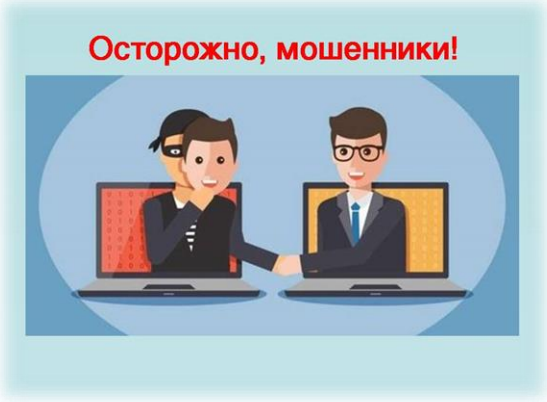
Как не дать обмануть себя в Интернете

**Краснодар
2021**

Дорогие ребята, мы хотим вам дать несколько советов, как избежать неприятностей в Интернете и не попасться на фишинг.

Фи́шинг (от английского *fishing* — рыбная ловля, выуживание) — интернет-мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей: логинам, паролям, данным кредитных карт, номерам телефонов, паспортным данным и другой личной информации. Преступники достаточно умело играют на психологии своих жертв.

Например, с помощью взлома соцсетей через специальные сервисы мошенники получают доступ к списку контактов, и вы можете получить СМС с "номера родителей". В сообщении злоумышленники просят от лица мамы или папы перевести им деньги. В этом случае необходимо перезвонить родителям и убедиться, что это сообщение отправили именно они.



Если вы играете в онлайн-игры, участвуете в конкурсах в Интернете, то мошенники могут прислать сообщение, что вы выиграли ценный приз (смартфон, ноутбук, планшет и др.) и попросить для доставки приза сообщить домашний адрес и номер телефона. После этого перезванивают "представители компании" и предлагают оплатить доставку или налог за подарок. Понятно, что после того как вы переведёте деньги для доставки приза, никакого подарка вы не получите.

Мошенники также могут заблокировать ваш аккаунт и предложить разблокировать его после отправки СМС на указанный номер, а потом спишут с вашей карты крупную сумму денег.

Необходимо также опасаться вирусов, которые внедряются в компьютер и подменяют настоящую страницу "Яндекс", "ВКонтакте", "Одноклассники" подложной, на которой предлагается ввести свои имя и пароль. Но после этого отображается иная страница, где говорится уже о необходимости "подтверждения" учётной записи через отправку СМС на короткий номер. Таким образом мошенники не только могут снять денежные средства с вашего счёта, но и получат логин и пароль от указанных популярных ресурсов, что позволит им в дальнейшем отправлять от вашего имени сообщения вашим друзьям о переводе денег якобы для вас.

Хорошим примером в этом отношении может служить целая эпидемия сетевого мошенничества, связанная с прошедшим недавно чемпионатом мира по футболу. Мошеннический сайт предлагал посетителям скачать электронный билет на чемпионат. На самом деле вместо билета пользователь получал банковского "троянца" — пробравшись в систему, вирус перехватывал личные данные, прежде всего финансового характера.