

ВНИМАНИЕ! ВАЖНАЯ ИНФОРМАЦИЯ.

ПАМЯТКА

«Профилактика мошенничеств и краж, совершаемых с использованием информационно-телекоммуникационных технологий, противодействие мошенническим схемам и противоправным действиям»

Уважаемые коллеги, родители (законные представители) учащихся, учащиеся ДЮЦ «Синяя птица»!

В настоящее время большое распространение имеют противоправные действия, направленные на обман, кражи денежных средств, похищение персональных данных граждан, так называемое IT-мошенничество.

IT - мошенничество - это виды мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий.

IT-преступления, или киберпреступления – это противоправные действия, совершаемые с использованием информационных технологий. Они могут быть направлены против отдельных лиц, организаций или государств.

Тенденция развития информационных технологий в последнее время влечет повсеместное их вовлечение во многие сферы общественных отношений, что сказывается не только на удобстве для добросовестных пользователей, но и служит почвой для противоправной деятельности, выражающейся в незаконном обогащении, дискредитации граждан и государственных органов, распространении запрещенной информации, в том числе, идей экстремизма и терроризма



ОСНОВНЫЕ ВИДЫ МОШЕННИЧЕСТВА



ВЗЛОМ АККАУНТА

Если вы получаете сообщение с просьбой об одолжении денег или сборе средств для благотворительности, то убедитесь, что это реальный человек, спросите у него что-то, что знает только он, либо просто игнорируйте такие сообщения.



КЛИКБЕЙТ

Кликбейт – захватывающий заголовок, который прерывается на самом интересном месте, и вас отсылают читать продолжение в источнике. В большинстве случаев кликбейт относительно безопасен – скорее всего вас просто перенаправит на страницу с рекламными баннерами. Однако такие новости могут быть опасными, потому что туда можно вложить ссылку с опасным контентом.



ВЫИГРЫШИ

Баннер, картинка или плашка от браузера, где заявляется, что ваш IP-адрес был выбран в качестве победителя.



ПЛАТНЫЕ ОПРОСЫ

Если вы видите такие предложения, то обратите внимание на предлагаемую сумму, если вам предлагают заработать 25 тысяч рублей за опрос — это обман.



СПАМ

Такие письма почти гарантированно содержат в себе вирус. Вы получаете спам-письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные.



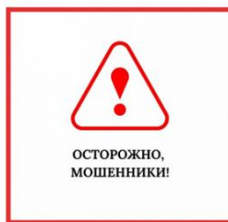
ДОКУМЕНТЫ И ФАЙЛЫ

В документах могут содержаться макросы. Они потенциально очень опасны. Поэтому если вы не пользуетесь макросами, то вам лучше отключить их исполнение в настройках офисных программ.



ФИШИНГ

Фишинг — один из видов интернет-мошенничества, основанный на принципах социальной инженерии, целью которого является обманом вынудить пользователя совершить необходимые злоумышленнику действия. Многие фишинг-атаки незамысловаты и легко выявляются. А некоторые могут быть весьма изощренными, поэтому следует проявлять здоровую дозу скепсиса, чтобы отсеивать подозрительные письма, ссылки и сообщения. Чтобы не попасться на типовые фишинг-атаки, руководствуйтесь приведенными ниже рекомендациями.



Рекомендации для повседневной жизни

В последнее время участились случаи, когда аферисты создают фейковые аккаунты государственных служащих или руководителей органов государственной власти в мессенджере «Телеграм», вступают в переписку с гражданами от имени госслужащих с целью узнать их персональные данные, звонят, придумывая различные методы выманивания информации.

Также вымогатели могут представляться операторами связи, сотрудниками банков, правоохранительных органов, онлайн-портала «Госуслуги». Несмотря на то что внешне они очень похожи на настоящий, при внимательном рассмотрении можно заметить, что наименование сайта в адресной строке отличается от официального домена.

ВАЖНО! Настоящий сайт «Госуслуги», а также официальные сайты финансовых организаций в популярных поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

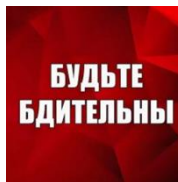
Будьте бдительны и внимательны! Помните: что бы ни говорили мошенники, их цель – выманить персональные данные, обмануть и ограбить человека.

- Всегда проверяйте информацию, общайтесь только через официальные каналы и сайты. Если вы получаете звонок или сообщение от кого-то, кто представляется сотрудником банка, силовых структур или органов власти, перезвоните на официальный номер, чтобы убедиться в подлинности обращения.

- Никогда не переводите деньги незнакомым людям, особенно если они просят сделать это срочно. Мошенники часто используют тактику давления, чтобы заставить вас действовать быстро и без размышлений.

- Установите на мобильное устройство антивирус и программу, которая предупреждает о том, что звонят мошенники, отмените онлайн-кредитование на большие суммы.

ВАЖНО! Если вы уже стали жертвой мошенничества, сообщите об этом в правоохранительные органы, оповестите свой банк и заблокируйте все счета и кредитные карты, а также поменяйте пароли для всех своих онлайн-аккаунтов. Вымогатели могут вновь связаться с вами, пытаясь получить дополнительную информацию или деньги.



ПОМНИТЕ ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ!

- Доверяйте только официальным источникам информации, сохраняйте бдительность и не поддавайтесь на провокации.
- Не указывайте личную информацию в открытых источниках. Адреса, даты рождения, номера телефонов: ваши и членов вашей семьи. Всё это может помочь мошенникам узнать пароль или секретное слово, взломать ваши аккаунты и получить доступ к деньгам и данным;
- Меняйте пароли не реже, чем раз в полгода. «Я вообще не меняю пароли, и меня ни разу не взломали. Зачем начинать?» – спросите вы, и это будет ошибка выжившего.
- Соблюдая правила, вы усложните работу преступникам, ведь никто не знает, когда на его деньги и данные может начаться охота;
- Не используйте одинаковые пароли для всех ваших аккаунтов.
- Не давайте мошенникам ключ от всех дверей. Мошенник, узнавший пароль от одного вашего аккаунта, сразу же попробует открыть этим ключом остальные ваши кабинеты, и он подойдёт. Не рискуйте всем и проявите фантазию, придумывая новые комбинации;
- Используйте режим инкогнито в браузере, когда работаете за чужим компьютером, заходите в свои аккаунты и вводите личную информацию. Когда вы закроете вкладку браузера, ваши пароли и данные не сохранятся, а выход из всех аккаунтов произойдёт автоматически;
- Исключите двухфакторную аутентификацию во всех ваших аккаунтах, потому что такой тип защиты надёжнее уберёжет вас от атак мошенников – чтобы взломать ваш аккаунт, им придётся преодолеть двойной барьер. И это будет непросто;
- Важно помнить, что IT-преступность – это серьёзная проблема, которая требует внимания и принятия мер для защиты себя и своих данных!

