# Как обезопасить себя в интернет – пространстве

Цифровое пространство – это не только полезная информация или обучающие игры. Там есть еще телефонное и онлайн-мошенничество, взломы аккаунтов, зловредное программное обеспечение. В сетях, опутавших мир, каждый рискует - стать жертвой преступников или быть втянутым в совершение преступления. Кстати, сколько бы вам ни было сейчас лет, обратите внимание на свои цифровые следы. Может, на онлайн-просторах вы рассказали о своих увлечениях и хобби, указали настоящий возраст, имена родственников, выложили фото с обстановкой квартиры? Если это так, то вы уязвимы.

Защита от киберпреступлений имеет две главных составляющих: это технические средства (антивирусные решения, блокировщики звонков – то, что можно установить на любое устройство) и нетехнические, связанные с всеобщим информированием, образованием.

Особенность общения в виртуальном мире заключается в том, что многие из нас больше доверяют виртуальным собеседникам, чем реальным. Хотя лучше бы обсудить какую-то тему с родителями, с тем, кто может дать дельный совет. Тогда мы не имели бы столько случаев вымогательства денежных средств у несовершеннолетних. Помните всегда и о том, что надо семь раз подумать, совершая онлайн-покупки: почему кроссовки стоят в два раза дешевле? Включайте критическое мышление.

Злоумышленники могут обмануть вас и другим образом, т.е. принудить к противоправным действиям. Они могут свести все к тому, что за какое-то злодеяние вам «ничего не будет», что вас «никто никогда не поймает». Между тем уголовная ответственность в нашей стране наступает по ряду преступлений с 14 лет. Все потому, что преступность очень сильно молодеет, растет число несовершеннолетних, которые привлекаются к ответственности. Многие подростки стремятся к финансовой независимости. Но некоторые в этом стремлении, к сожалению, обжигаются. Предложения с легким, быстрым и большим заработком необходимо игнорировать. На протяжении нескольких лет фиксируется огромное количество случаев, когда несовершеннолетние открывали в банках счета, привязывали к ним карты и за символическую плату передавали их данные третьим лицам, а те использовали информацию для своих преступных махинаций. По статье 222 Уголовного кодекса за изготовление для сбыта или сбыт банковских платежных карточек, а также за совершенное из корыстных побуждений незаконное распространение реквизитов карточек либо аутентификационных данных, предусмотрено наказание штрафом, или ограничением свободы на срок до пяти лет, или лишением свободы на срок до шести лет. Когда приходит время отвечать за поступки, подростки уверяют: они не подозревали, что совершают противоправные действия.

На вас могут оформить банковскую карту, номер телефона или дать попользоваться ими на какое-то время. Это нужно преступникам для отработки их преступных схем. Но фигурировать в деле будет ваше имя, значит, вам в случае поимки придется держать ответ перед законом. Чей-то удачный криминальный опыт может дать ложное успокоение, но надо также помнить, что все следы остаются в сети надолго.

Высказывание старшего координатора по защите детства ЮНИСЕФ в Беларуси Дмитрия Шилина:

- Интернет - не просто общение, не просто покупки, не просто игры. Здесь можно потерять имущество, здоровье или даже жизнь. При неправильном использовании цифровых технологий они могут нанести серьезный вред. Вы наверняка знаете, что такое буллинг. Это травля, когда все на одного... По данным опросов 40 процентов детей общались в интернете с незнакомыми людьми. Более 30 процентов сталкивались с запугиванием или травлей. 9 процентов учеников 5–7 классов и 18 процентов учеников 8–11 классов подвергались насилию со стороны людей, с которыми знакомы через интернет. При этом не все доверяют такую информацию родителям.

Когда вы безопасно ведете себя в интернете, то вы защищаете свою семью, потому что через вас преступники могут нанести вред вашим близким. Если будете подсказывать родителям, как вести себя безопасно, то они тоже смогут эффективнее защищать вашу семью.

Что поможет чувствовать себя безопасно в интернет – пространстве:

- обратите внимание на настройки приватности в соцсетях и на популярных платформах;
- используйте надежные и уникальные для всех аккаунтов пароли: минимум 12 символов с буквами в разном регистре, цифрами и спецсимволами;
- настройте двухфакторную авторизацию в тех сервисах, которые это позволяют;
- скачивайте приложения только из официальных магазинов и периодически проверяйте, какие программы установлены на устройстве;
- не переходите по сомнительным ссылкам в почте, мессенджерам и соцсетях, даже если их прислали знакомые;
- внимательно проверяйте название сайта в адресной строке перед вводом своих личных или платежных данных;
- установите надежное защитное решение;
- не выкладывайте большое количество данных о себе;
- если столкнулись с кибербуллингом, не вступайте в диалог с обидчиком, заблокируйте его, сообщите об этом администраторам площадки