**День защиты детей: как обезопасить ребенка от киберугроз**

С середины прошлого века, а точнее с 1950 года, 1 июня традиционно отмечается Международный день защиты детей. Это замечательный повод поговорить не только о радостях детства, но также обратить внимание на опасности, которые подстерегают детей и их родителей в современном мире.

Вирусы и трояны, фишинг и кибербуллинг: все эти опасные термины неразрывно связаны с источником знаний и развлечений – Интернетом. По словам заместителя управляющего Отделением Курск Банка России Александра Устенко, дети гораздо более уязвимы к таким угрозам, ведь они далеко не всегда знают об опасностях сети и зачастую не могут правильно оценить риски. Поэтому главная задача родителей – защитить своего ребенка, как минимум, вооружив его необходимыми знаниями.

Многие школьники используют банковские карты, привязанные к счету родителей или оформленные на себя (если у них уже есть паспорт). Часто через детей мошенники пытаются добраться до денег взрослых. Чтобы втереться в доверие ребенка, в ход идут обкатанные схемы. Вот пять самых распространенных уловок мошенников.

**Стань самым крутым в игре!**

Для обмана хакеры часто используют онлайн-игры. В виртуальном мире бдительность ослабевает, игроки могут не заметить подвоха и попасться на обман. Например, на предложение «выгодно купить» объекты для игры на фейковом сайте, пройдя по предлагаемой ссылке.

«Подростков заманивают низкими ценами и «уникальными акциями» в онлайн-играх. Надо заметить, что в подобные ловушки могут угодить не только дети, но и взрослые», – отмечает Александр Устенко.

**Заработай на мечту прямо сейчас!**

Для того, чтобы ребенку из своих карманных денег накопить, например, на новый гаджет, необходимы, как минимум, время и терпение. Тут же в виртуальном пространстве находятся «доброжелатели», с радостью готовые помочь.

Они размещают в интернете множество объявлений о быстром и легком заработке. Мошенники могут убедить подростка вложить деньги в «сверхприбыльный проект» (а по факту — в финансовую пирамиду), предлагают приводить друзей. До выплат вкладчикам дело обычно не доходит. Собрав деньги как можно большего числа людей, организаторы исчезают.

Порой жулики предлагают «быстро заработать», просто зарегистрировавшись на сомнительном сайте. Надо только выполнять задания или делать букмекерские ставки. Для вывода «заработка» они просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках махинаторов.

«Обещания молниеносной прибыли — это всегда тревожный знак. Если подросток хочет купить дорогую вещь, обсудите с ним, как достичь этой цели. Иногда ребенок может сам накопить необходимую сумму полностью или хотя бы ее часть. Быстрее достичь намеченного поможет финансовый план, его можно составить самостоятельно или вместе с родителями. Если копить придется долго, то лучше положить деньги на банковский вклад под процент», – советует Александр Устенко.

**Если друг оказался вдруг**

Несмотря на то, что эта мошенническая схема давно известна, она до сих пор продолжает приносить прибыль аферистам. Попадаются на нее как взрослые, так и подростки. Киберпреступники взламывают аккаунты в соцсетях, а затем от чужого имени рассылают сообщения по списку друзей. Начинают разговор с банального «как дела?» и практически сразу переходят к жалобам на жизнь и просят в долг. Или со словами «смотри, как ты вышел на этих фотках» вместо ссылки на фотографии присылают вредоносный вирус. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских. Могут быть и более сложные махинации.

Прежде чем выполнять все, о чем просит «приятель», лучше перезвонить ему и уточнить, действительно ли нужна помощь. Скорее всего, он не в курсе переписки. Но чем раньше он узнает о случившемся, тем быстрее предупредит остальных, что его аккаунт взломали. Защититься от вредоносных ссылок помогут антивирусы, которые можно установить на всех гаджетах. Для безопасности маленьких детей также можно настроить программы родительского контроля.

**О, счастливчик!**

Мошенники рассылают письма и сообщения о нежданном выигрыше, или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку приза или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого предлагается пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь теряет деньги.

Если организаторы конкурса просят что-либо оплатить, это повод, как минимум, насторожиться. Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что это не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах). Стоит проверить на официальной странице блогера, действительно ли он рекламирует этот конкурс, или он тоже стал жертвой мошенников.

**Давай дружить!**

Мошенники часто скрываются под маской интересных собеседников на форумах и в группах в соцсетях. Они заводят с подростком виртуальную дружбу на почве общих интересов и втираются в доверие ради будущей выгоды. Когда контакт налаживается, они выдумывают различные предлоги, чтобы получить необходимую им информацию. Например, просят ребенка прислать фотографии банковских карт или паспортов родителей. Этих данных может оказаться достаточно, чтобы украсть деньги со счета или оформить кредит на чужое имя.

**Советы от Александра Устенко:**

«Чтобы обезопасить ребенка, нужно как можно раньше обсудить с ним правила разумного финансового поведения. Невозможно представить жизнь современного человека без гаджетов, ребенку же разобраться в теме финансов помогут специальные мобильные приложения. Есть также подходящие подборки книг про деньги и экономику.

Подключите СМС или push-оповещения ко всем банковским картам, так вы сразу заметите подозрительные покупки.

Не стоит переводить на карту ребенка крупные суммы. Кроме того, можно ограничить суммы списаний или количество операций по карте в день, чтобы мошенникам не удалось украсть с нее все деньги разом».