КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

191311, Санкт-Петербург,
пл. Растрелли, д.2
тел.: (812) 539-42-00, факс: (812) 539-51-75
www.kis.lenobl.ru, e-mail: kis@lenreg.ru

30.09.2022 №22-04-18-2841/2022

На № _____от_____

Председателю комитета общего и профессионального образования Ленинградской области

Ребровой В.И.

О мероприятиях по обеспечению информационной безопасности детей

Уважаемая Вероника Ивановна!

В соответствии с п.2 протокола заседания постоянной комиссии по строительству, транспорту, связи и дорожному хозяйству от 8 сентября 2022 года Законодательного собрания Ленинградской области Комитет цифрового развития Ленинградской области направляет перечень региональных мероприятий, направленных на обеспечение информационной безопасности детей.

Приложение: Перечень региональных мероприятий по обеспечению информационной безопасности детей на 4 л. в 1 экз.

Первый заместитель председателя
Комитета цифрового развития
Ленинградской области

Подлинник электронного документа, подписанного ЭП, хранится в Межведомственной системе электронного документооборота Правительства Ленинградской области
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 56096B8E2F32172EA440E4E819B7F7AA
Владелец: Попов Александр Юрьевич
Действителен с 18-07-2022 до 11-10-2023

А.Ю. Попов

исп. Петров Н.В.. +7(812)539-42-05, 1504

Перечень региональных мероприятий по обеспечению информационной безопасности детей

1. Подготовить подборку материалов о способах мошенничества в Интернет, ориентированных на детей (в т.ч. в онлайн-играх), правилах безопасного пользования Интернет, безопасной оплаты покупок. Материалы разместить на официальных сайтах КОиПО, КЦР.
2. Ссылки на материалы разместить на страницах школ, других страницах, часто посещаемых детьми.
3. На базе материалов разработать сценарии классного часа (семинара - в зависимости от возраста), сообщения для родительского собрания, посвященных проблеме информационной безопасности детей, довести до учителей, включить материалы в школьные программы.

Материалы должны содержать организационные и просветительные мероприятия, проводимые со стороны родителей и учителей.

К организационным мероприятиям относятся организация безопасного режима работы на компьютерах и мобильных устройствах, а также финансовый мониторинг.

Организация безопасного режима для ребенка.

На многих компьютерах и мобильных устройствах предусмотрен безопасный «Детский режим». Также можно настроить ограничения с помощью домашнего роутера – обычно эта функция называется «Родительский контроль». Еще один вариант – использование специальных детских расширений для браузеров. Любой из перечисленных выше вариантов сводит к минимуму вероятность того, что ребенок попадет на опасный сайт. И, конечно, заведите ему собственную учетную запись.

Финансовый мониторинг.

Подключение СМС или push-оповещения ко всем банковским картам, которые используют дети, что обеспечивает контроль подозрительных покупок.

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.

К просветительным мероприятиям относятся мероприятия по разъяснению и предупреждению возможных действий хакеров и мошенников в отношении детей.

Создание фейковых страниц для онлайн-покупок.

Хакеры любят онлайн-игры не меньше, чем дети, но у них на это свои причины. В виртуальном мире бдительность ослабевает, и игроки могут не заметить обмана и клюнуть на уловки мошенников. Например, на предложение «выгодно купить» объекты для игры на фейковом сайте.

Игроков заманивают низкими ценами и «уникальными акциями». И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые.

Прежде чем вводить где бы то ни было персональные данные, пароли, коды или реквизиты банковской карты, удостоверьтесь, что это не мошенническая страница.

Предложения быстрого обогащения.

Если подростку не хватает карманных денег на модный телефон и терпения, чтобы на него накопить, мошенники с радостью ему «помогут». Они размещают в интернете множество объявлений о быстром и легком заработке. Но зачастую в таких случаях внезапно разбогатеть удается только самим махинаторам.

Мошенники могут убедить подростка вложить деньги в «сверхприбыльный проект» (спойлер — в финансовую пирамиду). До выплат вкладчикам дело обычно не доходит. Собрав деньги как можно большего числа людей, организаторы исчезают.

Порой обманщики 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.

Завлекания «выигрышами» в конкурсах.

Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш, 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 надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

Если организаторы конкурса просят что-либо оплатить, это повод насторожиться. Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что организаторы — не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах).

Когда конкурс рекламирует блогер, стоит проверить на его официальной странице, действительно ли он рекламирует этот розыгрыш. Возможно, он тоже стал жертвой мошенников.

Просьбы о помощи от имени друзей в соцсетях.

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 «лови фотки с дня рождения!» вместо ссылки на фотографии присылают вредоносный вирус. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских карт. 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.

Набиваются в друзья на тематических форумах

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, мошенники 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.

Чтобы обезопасить ребенка, нужно как можно раньше обсудить с ним правила разумного финансового поведения. Если он жить не может без гаджетов, то разобраться в теме финансов ему также помогут специальные мобильные приложения, а для любителей почитать есть подходящие подборки книг про деньги и экономику.

Относительно законодательных ограничений в целях обеспечения безопасности жизни, охраны здоровья и нравственности детей, защиты их от негативных воздействий компьютерных игр, считаем, что действующих законодательных ограничений изложенных в Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» с учетом последний изменений внесенных

Федеральным законом от 14.07.2022 № 277-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» достаточно с учетом предложений Комитета касающихся социального развития и воспитания.