Банк России назвал Топ-5 угроз, которые подстерегают детей в киберпространстве

В Международный день защиты детей, который отмечается 1 июня, принято говорить о безопасности подрастающего поколения в разных сферах, и конечно, нельзя обойти стороной интернет, где кибермошенники охотятся за деньгами детей, подростков и их родителей. Эксперты тамбовского отделения Банка России рассказали о пяти наиболее популярных угрозах, которые подстерегают детей в сети.

1. Подделки

Основной прием кибермошенников в сети – это фишинг. Аферисты создают подделки на сайты, которые пользуются популярностью среди детей и подростков, как правило, это онлайн-магазины компьютерных игр, техники и аксессуаров по низким ценам, развлекательные порталы, каналы в мессенджерах. Если ввести данные карты на фишинговом сайте, мошенники могут получить доступ к деньгам на счете жертвы и списать их. Современные кибераферисты также создают очень похожие на оригинал поддельные приложения, они могут содержать вредоносный вирус, который откроет доступ мошенникам к данным на устройстве, может читать коды из СМС, что также может привести к хищению средств.

2. Овершеринг

Общение современных детей и подростков большую часть времени происходит в сети, где на обозрение друзей выкладываются посты и фото, отражающие практически всю жизнь – от съеденной на завтрак еды до дорогих путешествий. Всю информацию, которую выкладывают дети в сеть, могут использовать в своих схемах мошенники. Геолокации, даты событий, обстановка в квартире, состав семьи, фото документов, билетов – любая деталь может стать поводом для разного рода атак, как массовых, так и целевых.

3. Излишнее доверие

Дети привыкли развлекаться и расслабляться в сети, поэтому само виртуальное пространство и собеседники здесь воспринимаются ими с доверием. К сожалению, этим доверием и невнимательностью могут воспользоваться аферисты. Мошенники взламывают аккаунты в социальных сетях и по списку друзей раскидывают сообщения с просьбой перевести деньги, кроме того, со взломанного аккаунта аферисты могут прислать вредоносную ссылку с каким-нибудь интригующим предисловием, вроде «ответы на ОГЭ», «оцени мою фотку в конкурсе» и тому подобное. Перейдя по ссылке, ребенок может загрузить на свой гаджет вирус или ввести конфиденциальные данные на фишинговом сайте. Кроме того, на тематических площадках и форумах к ребенку могут втереться в доверие аферисты под маской ровесников. Такой «виртуальный друг» может провоцировать ребенка под «благовидными» предлогами сообщить ему данные карты своей, а также и родителей.

4. Обратная сторона технологических новинок

На волне популярности нейросетей, в том числе среди молодежи, появились фишинговые ресурсы якобы предоставляющие доступ к работе с нейросетью. Сначала доступ для нее бесплатный, а затем становится платным, и пользователи вводят платежные данные на сайте мошенников, которые похищают деньги.

Аферисты могут заманивать и в криптопирамиды, используя дипфейки. Они могут взломать канал популярного тематического блогера и разместить здесь рекламу финансовой пирамиды, используя технологию дипфейк, чтобы вызвать максимальное доверие подписчиков. Эта реклама будет висеть, пока владельцам не удается отбить канал обратно и удалить видео, за это время доверчивые пользователи канала могут перевести деньги аферистам».

5. Желание легкого заработка

Подростки ищут подработку в сети, откликаются на вакансии, предлагающие легкий заработок, и здесь могут столкнуться с уловками мошенников. Аферисты создают фишинговые сайты, имитирующие платное прохождение опросов, заполнение анкет, и другие способы легко заработать, а для получения денег предлагают ввести данные карты, опустошая ее. Опасность представляют также и предложение подросткам быть посредниками при переводе денег со счета на счет за процент. Таким образом ребенка могут втянуть в нелегальные схемы по движению средств, то есть стать дроппером, за что можно получить уголовное наказание.

«Предупредите ребенка о том, что аккаунты в соцсетях должны быть закрыты от посторонних, делиться личной информацией нужно осторожно, нельзя переходить по подозрительным ссылкам, а также соглашаться на предложения, касающиеся денег от виртуальных собеседников, на все устройства нужно установить антивирус. Перед покупкой в сети нужно удостовериться, что сайт настоящий, проверить его название, перед оплатой убедиться в наличии в адресной строке значка закрытого замочка и надписи https, сохранить адреса регулярно используемых порталов в закладках браузера, перед покупкой на незнакомом сайте стоит обратить внимание на наполненность ресурса, отсутствие ошибок. К сожалению, все это не панацея от возможности попасть на фишинговый сайт, поэтому универсальным советом можно назвать такой: для оплаты в сети следует завести отдельную или виртуальную карту, класть на нее деньги непосредственно перед покупкой или установить лимит трат» – напомнил основные правила эксперт отдела безопасности тамбовского отделения Банка России Андрей Башканков.