Вишинг, фишинг, с чем ещё могут столкнуться наши дети?

В двадцать первом веке информационные технологии очень плотно вошли в наш мир и во много они позволяют облегчить нашу жизнь, но на ряду с положительными тенденциями возникает и ряд отрицательных. В первую очередь под угрозой находятся дети, которые с малых лет погружаются в современные возможности информационных технологий и могут стать, как жертвами «кибер-преступников», так и сами стать на тропу совершения противоправных деяний.

Вишинг – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами мошенники выясняют сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

Фи́шинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Груминг – это вхождение взрослого человека в доверие к ребенку с целью сексуального самоудовлетворения. Злоумышленник дистанционно нащупывает связь с ребенком через социальные сети, мессенджеры, онлайн-игры, электронную почту. Затем может вынудить ребенка прислать фотографии интимного характера, вовлечь в изготовление порнографических материалов, склонить к интимной встрече в реальности.

Кибербуллинг – травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить травлю могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди. Эта форма психологического террора может принимать разные обличия: оскорбления через личные сообщения, публикация и распространение конфиденциальной,

провокационной информации о жертве; физическая агрессия и так далее. Причины кибербуллинга: чувство превосходства, зависть, чувство превосходства над соперником, чувство собственной неполноценности, самореализация. Особо следует отметить способ воздействия запрещенным контентом. Ребенку могут показывать порнографические материалы, нанося ущерб психике, так как изображенное со временем перестанет восприниматься ребенком как аморальное поведение.

Угроза нового времени – так называемые группы смерти. И хотя обычно создателями таких групп являются сами подростки (цель – «хайп», жажда острых ощущений, желание доминировать и управлять другими), в подобных группах создается благоприятствующая атмосфера для культивирования суицидальных намерений.

Сегодня не только дети могут стать жертвами кибер-преступлений, но и сами быть непосредственными участниками, забывая об уголовной ответственности, которая может их ожидать. Одним из видов таких преступлений является Сватинг – заведомо ложный вызов полиции, аварийно-спасательных служб, путем фальшивых ложных сообщений об опасности (например, о минировании, убийствах, захвате заложников). Стоит отметить, что ответственность за это преступление наступает с 14 лет. Наказание – штраф, арест, ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет. В случае, если сообщившему о ложном минировании, не исполнилось 14 лет, наступает административная ответственность родителей, а ребенка ставят на учет в инспекцию по делам несовершеннолетних. (ред.)

Также пользуясь интернетом, дети могут начать посещать сайты различной тематики, в том числе и хакерской, где можно скачать и научиться пользоваться вредоносным программным обеспечением для получения несанкционированного доступа к аккаунту пользователей. За совершения данного рода правонарушений предусмотрена уголовная ответственность в виде штрафа, или ареста, или ограничения свободы на срок до трех лет, или лишения свободы на тот же срок.

Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной

средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Советоваться с родителями. Если ребенок хочет зарегистрироваться на каком-либо сайте, создать профиль в социальной сети и выложить свои фотографии, лучше перед этим посоветоваться с родителями. Взрослый человек сможет лучше проанализировать ситуацию и понять, опасен ли сайт, а также помочь выбрать снимки, которые можно выложить на всеобщее обозрение.

Установить дистанционный контроль.
Функция «родительского контроля» – это и как специализированное ПО, так и услуги провайдера, которые включает в себя стандартный набор функций. А именно:

ограничение времени нахождения ребенка в сети;

ограничение времени пользования компьютером;

возможность создания графика с допустимыми часами работы в течение дня;

блокировка сайтов с запрещенным контентом;

ограничение на запуск приложений (например, игр и иных приложений) и установку новых программ;

Беречь личные данные.
Даже если ребенок думает, что хорошо знает человека, с которым общается онлайн, не нужно рассказывать подробности о себе и о родителях. Номер телефона, адрес, номер школы и класса, место работы родителей и их график, время, когда в квартире нет взрослых, а также данные из документов, номера банковских карт – такую информацию ни в коем случае нельзя передавать другим людям.

Не делиться информацией о знакомых.
Правило, приведенное выше, распространяется и на других людей. Не нужно рассказывать про друзей и одноклассников, сообщать, где они живут и учатся, какие кружки посещают. Нельзя показывать их фотографии – ни выкладывать их в своих профилях в социальных сетях, ни тем более в частной переписке.

Если хочется выложить групповое фото с праздника или тренировки, сначала стоит обсудить это с теми, кто изображен на снимке. И лучше, если они сообщат родителям, что такое фото публикуется в интернете.

Фильтровать информацию.
Мошенники активно используют интернет в своих интересах. Они могут обманывать людей и манипулировать ими, давя на жалость или страх. Поэтому надо научиться скептически относиться к любой информации, размещенной в интернете, и не доверять слепо всему, что там пишут.