Эксперт «Лаборатории Касперского» в эфире проекта «Суббота онлайн» рассказал о мошенничестве в сети

30.06.2020

Как защитить себя и свою семью от онлайн-мошенников, какие техники используют злоумышленники, чем отличается фишинг от вишинга, и как не попасться на удочку скамеров? Обо всем этом подробно рассказал руководитель направления по детской онлайн-безопасности «Лаборатории Касперского» Андрей Сиденко в проекте «Суббота онлайн» учебного центра «Профессионал».

С чем можно столкнуться в интернете

В виртуальном мире существуют вполне реальные опасности, они могут коснуться и взрослых, и детей. Пять основных видов мошенничества в сети, на которые следует обратить внимание:

- фишинг — попытка принудить человека к нежелательным действиям или выманить конфиденциальные данные;
- кража личности — незаконное использование чужих персональных данных, взлом аккаунтов;
- онлайн-мошенничество, направленное на быстрое получение денег обманным путем;
- рассылка СМС со ссылками на фейковые сайты;
- вишинг — мошенничество с помощью телефонных звонков.

«Злоумышленники используют фишинговые сайты, очень похожие на действительно существующие сервисы, например, на сайты банков, но на самом деле созданные для хищения персональных данных, логинов и паролей. В соцсетях крадут целые страницы и от имени владельца делают рассылки, вымогая деньги. Скамеры создают лотереи и викторины для быстрого получения денег. Ключевой целью всех схем является доступ к персональным данным и получение дальнейший выгоды для себя», — рассказал Андрей Сиденко.

Как это работает

Письмо с ссылкой на сомнительный сайт можно обнаружить в своей почте. Как правило, такие письма очень похожи на рассылку известных брендов или интернет-магазинов и содержат кнопку перехода на фишинговый сайт. Выдает «подделку» адрес отправителя, который отличается от настоящего.

Через мессенджер можно получить сообщение о счастливом выигрыше ценного подарка или о

бесплатном бонусе в честь дня рождения компании. Ссылка в сообщении также ведет на фейковый сайт, где можно попасться на удочку мошенников.

По такой же схеме работают поддельные аккаунты в социальных сетях, новости и рекламные объявления о мнимых социальных выплатах.

> *«Жертвами фейковых государственных выплат чаще всего становятся пенсионеры и граждане, получающие социальные выплаты. Мошенники подделывают официальные сайты госучереждений с целью обмана и получения денег, поэтому ссылки рекомендуется перепроверять. В первую очередь нужно обращать внимание на доменное имя, адрес ресурса и не стесняться открывать поисковик, чтобы уточнить информацию в официальных источниках. Также можно позвонить по горячей линии и узнать всю информацию о предлагаемых выплатах»,* — рекомендует эксперт.

Еще одна разновидностей мошенничества — «беспроигрышная» лотерея и получение призов за опросы. Она не требует ни детальной проработки, ни подготовки. Создаются простые страницы с опросом и предлагается оплатить «закрепленный платеж» или комиссию при получении приза.

Очень часто для обмана используются реальные сайты объявлений. Подростки интересуются последними моделями смартфонов, и этим пользуются злоумышленники.

> *«Самая распространенная схема — размещение фотографии телефона с подписью: «Подарили точно такой же, поэтому отдам бесплатно». А дальше все очень просто: телефон предлагают отправить почтой, но для этого нужно оплатить налог либо пересылку. На предложение лично приехать за телефоном не соглашаются, ссылаясь на то, что живут очень далеко — просто так не доедешь»,* — рассказывает Андрей Сиденко.

Как защититься от злоумышленников

Многие мошеннические схемы очень просты и рассчитаны на невнимательность или неосведомленность пользователей. Соблюдение базовых принципов безопасного поведения в Интернете поможет не стать жертвой злоумышленников.

- Не переходите по ссылкам, которые от сомнительных источников.
- Никому не сообщайте свои персональные данные по телефону, в СМС или в письме.
- Не загружайте на свой компьютер файлы и архивы, прикрепленные к электронным письмам с незнакомых адресов. Это может быть зловредное программное обеспечение или вирусы.
- Внимательно смотрите на адрес сайта, на который вы заходите. Абсолютно не стыдно открыть соседнюю вкладку и проверить информацию по этой теме. Найти настоящий ресурс, посмотреть, как он выглядит, сравнить адреса и не переходить на сайт мошенников.
- Обновляйте браузер до последней версии и используйте антивирусное программное обеспечение.

Осторожно, социальные сети!

> *«Всегда нужно помнить, что любая публикация в социальной сети несет для человека очевидные последствия в реальном мире. Это относится к фотографиям, текстам и любым другим данным, которые размещаются в сети, поэтому внимательно относитесь к тому, что публикуют ваши дети, и какие они делают репосты»,* — советует эксперт.

Фотографии, размещенные в сети, уже не принадлежат автору. Они могут быть использованы кем угодно и где угодно, и это неконтролируемый процесс. Любой может сделать скриншот, разместить его в другом аккаунте и выдавать за свой контент. Этим могут воспользоваться и злоумышленники.

Андрей Сиденко рекомендует закрывать аккаунты детей в соцсетях, вместе с ними проверять настройки безопасности и объяснять детям, что добавлять в друзья стоит только знакомых людей, чтобы посторонние не могли видеть личную информацию.

> *«Обратите внимание на группы, в которых состоят ваши дети. Возможно, ребенок подписался на совершенно другую группу, с другим контентом, но со временем тематика сообщества может измениться, а контент стать вредоносным. Если ребенок сознательно не выходит из такой группы, поговорите с ним, спросите, почему ему нравится такой контент и обсудите вопросы безопасности»,* - советует эксперт по детской онлайн-безопасности.

Основные правила безопасного поведения в соцсетях, которые важно донести до ребенка:

- не публиковать слишком много личной информации о себе;

- не публиковать домашний адрес и не ставить точную геолокацию;
- закрыть личный аккаунт для сторонних пользователей;
- избегать ситуаций, в которых вы могли бы стать героем видеоролика, который попадет в соцсеть без вашего ведома.

«Объясните детям, что нужно несколько раз подумать, прежде чем сделать тот или иной пост. Пусть у ребенка срабатывает ценз: «А что бы сказала мама?» С другой стороны, такие публикации — повод поговорить со своими детьми о том, что их беспокоит», — отмечает Андрей Сиденко.

Как противостоять кибербуллингу

Травля в сети — это острая социальная проблема, которая затрагивает и детей, и взрослых.

Несмотря на то, что кибербуллинг существует в Интернете, он имеет очень серьезные последствия в реальной жизни: сильный стресс, снижение успеваемости и социальной активности, проблемы со сном, ухудшение здоровья. Дети зачастую не говорят родителям о такой проблеме, предполагая, что они ничем не помогут, а на самом деле помочь можно, и нужно обязательно защищать детей, когда они подвергаются психологическому давлению.

«Первое, что необходимо сделать, — заблокировать человека, от которого исходит угроза. Ни в коем случае не отвечать на его сообщения — зачастую инициатор травли именно этого и добивается. Сообщите о случившемся администраторам социальных сетей, фиксируйте сообщения, обязательно сохраняйте скриншоты страниц. В случае угрозы жизни и здоровью обратитесь в правоохранительные органы. Понятно, что ребенок сам этого не сделает, поэтому объясните ему, что вы рядом и готовы помочь», — рекомендует Андрей Сиденко.
