Приложение к письму

от\_\_\_\_\_\_\_\_\_№\_\_\_\_\_

**МОШЕННИКИ ПРОБУЮТ ДОБРАТЬСЯ ДО ДЕНЕГ РОДИТЕЛЕЙ ЧЕРЕЗ СМАРТФОНЫ ДЕТЕЙ**



ДЕТИ В ИНТЕРНЕТЕ, А ДЕНЬГИ РОДИТЕЛЕЙ ПОД УГРОЗОЙ

Согласно исследованиям Ipsos, 90–94% подростков имеют смартфоны, 93% регулярно используют компьютер. Ребенок, если скачает подозрительный софт, скорее всего, не распознает в нем шпионскую программу. Попав в гаджет вашего чада, она сможет передавать персональные данные злоумышленникам, отслеживать геолокацию и даже управлять приложениями в телефоне.

Многие школьники используют банковские карты, привязанные к счетам родителей, или пользуются общим с ними счетом. Дети вряд ли будут чистить свой гаджет и удалять неиспользуемые программы, поэтому может пройти много времени, пока кто-то из взрослых обнаружит неладное, а мошенникам это только на руку, через детей они могут получить выход на банковские счета родителей̆.

«ЛОВИ СЕКРЕТНУЮ ССЫЛКУ»

Дети любят играть в онлайн-игры. Но везде поджидают свои опасности. Заигравшись, легко потерять бдительность. Так, нередки случаи, когда подростки в игровом чате получают предложения перейти по «волшебной» ссылке, чтобы получить внутриигровые предметы или усиление аккаунта. Ясное дело, что ссылка ведет на фишинговый сайт.

ОБЪЯВЛЕНИЯ О БЫСТРОМ И ЛЕГКОМ ЗАРАБОТКЕ МАНЯТ ПОДРОСТКОВ

Тема карманных денег актуальна для подростка всегда – и для аферистов тоже. Они с радостью «помогут», ведь надо всего лишь зарегистрироваться на нужном сайте и делать непыльную работу. А для вывода средств просят оплатить комиссию, завладев таким образом данными карты. Кроме того, подобными предложениями по схеме финансовой пирамиды изобилуют группы в соцсетях и Telegram-каналы.

ЧТОБЫ ПОЛУЧИТЬ КРУТОЙ ПРИЗ, ТРЕБУЕТСЯ ВСЕГО ЛИШЬ ОПЛАТИТЬ ЕГО ДОСТАВКУ

То же с сообщениями о внезапном выигрыше в лотерее или розыгрыше. Приз отдадут якобы после оплаты комиссии за доставку. Схема та же: подросток введет данные карты на «левом» сайте – и мошенники уже в его личном кабинете. Кроме того, действует схема «Коробка с сюрпризом»: за оплату в размере 200–1200 рублей пользователю предлагают открыть виртуальную коробку, где случайным образом в качестве подарка может выпасть, например, дорогая техника.

ЭТО НАДО СДЕЛАТЬ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РЕБЕНКА В СЕТИ

- Установите средства родительского контроля. С его помощью можно запретить просмотр контента и установку приложений, которые не подходят ребенку по возрасту.

- Установите антивирус. Программа будет блокировать установку подозрительного софта и предупредит ребенка о переходе по сомнительной ссылке.

- Проведите цифровой ликбез. Объясните ребенку, что многие в интернете выдают себя не за тех, кем являются. Изучите сами и затем покажите, каким образом можно заблокировать и внести в черный список нежелательного человека в соцсетях. Предупредите, что нельзя общаться с незнакомцами в чатах, кликать по сомнительным ссылкам и скачивать приложения из непроверенных источников. Расскажите, что принцип «доверяй, но проверяй» работает и в виртуальном пространстве. Даже если пишут друзья, не стоит бросаться выполнять их просьбы. Лучше сразу перезвонить и уточнить все вопросы лично. Ведь может оказаться, что они вам и не писали.

РУКОВОДИТЕЛЬ ЦЕНТРА ЦИФРОВОЙ ЭКСПЕРТИЗЫ РОСКАЧЕСТВА ПОЯСНЯЕТ:

– Сейчас у каждого человека есть не только общественная и частная жизнь, но еще и цифровая. И в интернет-пространстве ребенку тоже нужно объяснять, что такое хорошо и что такое плохо. Мы бы рекомендовали рассказать ему о фишинге. Когда злоумышленники пытаются выудить, словно на рыбалке, важную информацию, используя разные «крючки»: красивые обещания, просьбы помочь, сообщения о выигрышах и т. п.

Ребенок должен знать, что нельзя никому сообщать Ф.И.О., домашний адрес, реквизиты карт, пароли, ПИН-коды и прочие личные данные. Их нельзя разглашать и публиковать в интернете.

https://rskrf.ru/tips/eksperty-obyasnyayut/moshenniki-probuyut-dobratsya-do-deneg-roditeley-cherez-smartfony-detey/