БАНКИ – НЕ СКЛЯНКИ

КАК НЕ ОТДАТЬ МОШЕННИКАМ ДЕНЬГИ С БАНКОВСКИХ КАРТ

Ты спросишь, почему в детском журнале мы вдруг заговорили о таких взрослых вещах, как банковские карты? Да потому, что у многих ребят они тоже есть! Детские карты выпускают несколько российских банков. Родители кладут на них деньги – и ребёнок может оплачивать своей картой любые покупки. И личный кабинет на сайте банка завести, чтобы онлайн-покупки делать. Вот тут его и могут подстерегать мошенники. Много у нас ещё людей, которые хотят поживиться за чужой счёт.

КИБЕРВОРЫ

Сколько твоих одноклассников имеют смартфоны с выходом в Интернет? Наверняка почти все. Ну уж точно больше половины класса. А сколько пользуются разными мобильными приложениями? Тоже много! Эту любовь к мобильному интернету мошенники очень даже разделяют – ведь столько способов обмана можно придумать! Особенно в приложениях, к которым пользователи смартфонов привязывают банковские карты. Взрослым это очень удобно: за квартиру или налоги заплатить, деньги родным перечислить, оплатить покупку в интернет-магазине… Кстати, даже не все взрослые знают, какая опасность их тут подстерегает. Так что дай прочитать этот номер журнала и папе с мамой.

Итак, киберворы разработали вирус, который через Интернет прописывается в смартфоне и отправляет деньги с карты пользователя на счёт мошенников. При этом иногда даже эсэмэска не приходит о том, что со счёта списаны деньги. И через некоторое время пользователь видит, что денег-то на карте нет!

Что делать?

IT-специалисты предлагают разделить вход в интернет-банк на разные устройства. Например, приложение установлено на планшете, а код оповещения приходит на мобильный телефон. Кто-то посчитает это неудобным, зато такая мера обезопасит счёт.

ДАННЫЕ ДЕРЖИ В СЕКРЕТЕ

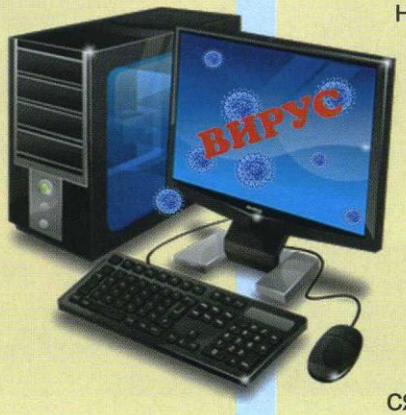
Другие мошенники пытаются выведать у пользователей данные банковской карты – номер счёта, логин и пароль входа в личный кабинет или платёжную систему, пин-код карты. Ты получал когда-нибудь смс-рассылки от какого-то банка? Читай их внимательно. И не верь сообщениям о том, что твой счёт заблокирован, или подобным им.

Рисунок с сайта: https://0.s3.envato.com

Предлагая перейти по ссылке, мошенники переводят тебя на сайт-дублёр (в адресе которого, например, одна буква или знак будут изменены, а всё остальное – как у вполне надёжного банка, а эту буковку-то можно и не заметить!). Сайт-дублёр сделан по образцу надёжного банка, так что пользователь не сразу и поймёт, что зашёл на ложный сайт! На странице будет вполне правдивое объявление – к примеру, об изменениях в системе безопасности. И просьба указать данные карты. Дальше за вас всё сделает мошенник.

Что делать?

Во-первых, всегда обращай внимание на название сайта. Если есть сомнения, покажи этот сайт взрослым. Во-вторых, проверяй, установлено ли защищённое соединение, прежде чем вводить пароли, номера карт, паспортные данные и другую личную информацию. Защищённое соединение в адресной строке имеет вид https://, а не http (о защищённости также свидетельствует значок амбарного замка на зелёном фоне рядом с адресной строкой). Ещё можно позвонить на горячую линию своего банка – её номер указан на самой банковской карте – и задать вопросы специалистам.



КОТ В МЕШКЕ

Многие люди стараются покупать что-то там, где это «что-то» стоит дешевле. Тем более что рекламы сайтов совместных покупок, бонусных и скидочных программ в Сети полно. Где-то продают реально дешёвые и качественные вещи, а где-то сидят мошенники, которые тоже не прочь пожить за чужой счёт. Банковский.

Итак, ты увидел объявление, где та штука, о которой ты давно мечтал, продаётся по нереально низкой цене. И телефончик указан. И рука сама тянется набрать номер – ведь до мечты один шаг! А там тебе говорят, что желающих много и если уж очень-очень хочется, нужно перевести задаток – часть стоимости товара. И вроде как потом продавец сразу тебе этот товар отправит или привезёт. И что? Очень не советуем тебе проверять, честен этот продавец или нет. Скорее всего, после получения задатка его телефон станет недоступен, а ты лишишься и денег, и мечты. На таких «наивных ромашках» мошенники целые состояния зарабатывают.

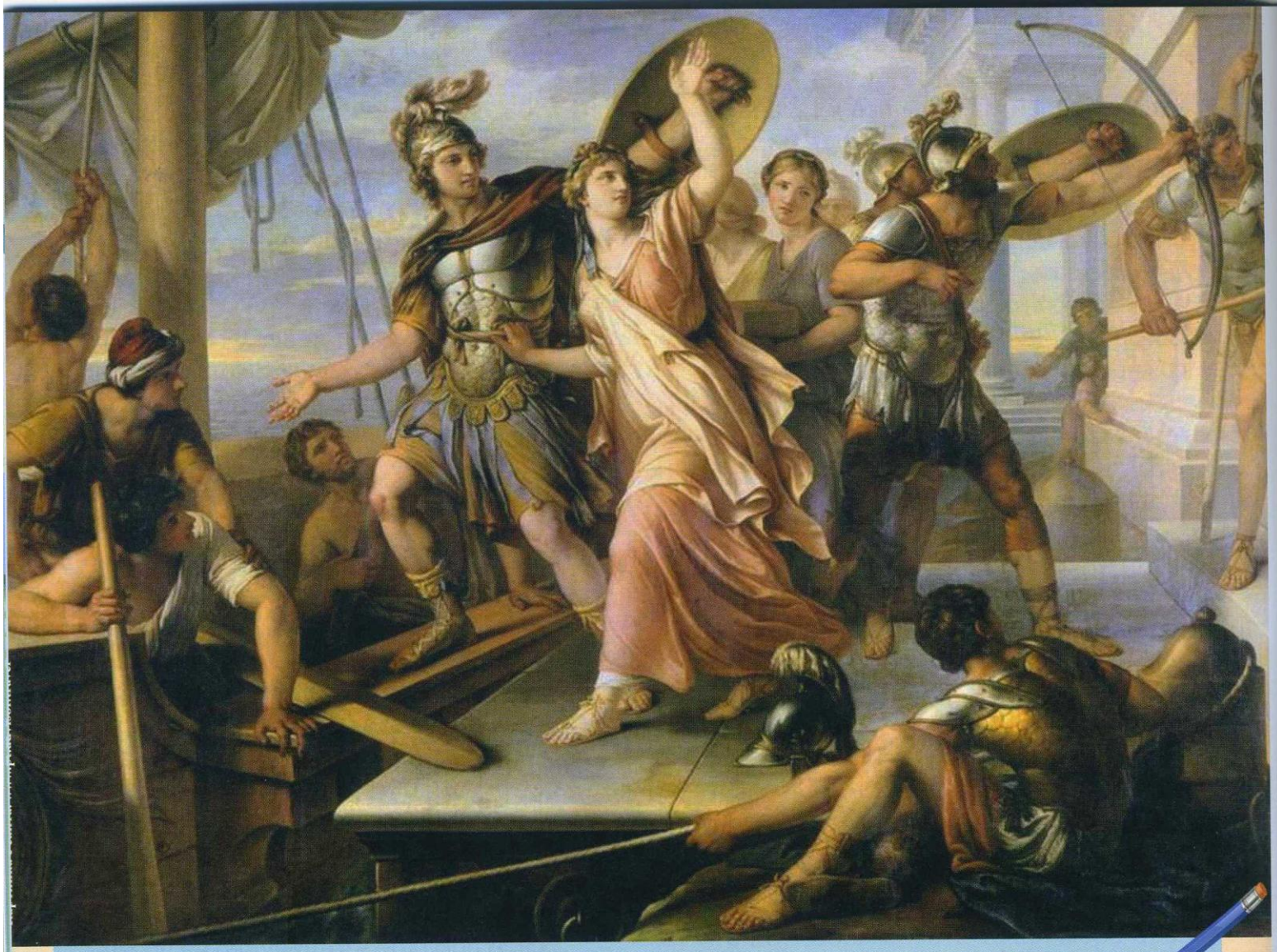
Что делать?

Прежде всего – слушать умных взрослых людей. УМВД России по Белгородской области предупреждает, что ни в коем случае нельзя сообщать данные банковской карты и переводить деньги незнакомым людям. Тем более за товар, который в глаза не видели. Так можно или кота в мешке купить (так говорят о ситуации, когда человек покупает что-то, не видя самой покупки и не подозревая, что ему могут подсунуть), или вообще ничего не купить, а без денег остаться. А покупать что-то нужно на проверенных сайтах или лично в магазине.

ОПАСНЫЙ ВИРУС

Ты, наверное, слышал о почтовых вирусах, которые распространяются через электронную почту и повреждают файлы в компьютере, смартфоне или планшете? Думаешь, с тобой такая беда никогда не случится? К сожалению, никто от этого не застрахован. Кроме внимательных людей, которые не открывают письма от незнакомцев.

Заражённое вирусом письмо прописывает его на твоём устройстве, а дальше всё зависит от типа вирусов. Одни могут повреждать файлы или всю операционную систему (то есть либо у тебя не будут открываться какие-то файлы, либо компьютер вовсе перестанет работать). Другие – передавать информацию с твоего компьютера или другого устройства другим людям, это так называемые вирусы-трояны. Названы они так по имени троянского коня. Помнишь этот эпизод из истории Древней Греции?



Картину шотландского живописца Гэвина Гамильтона «Похищение Елены» можно увидеть в Музее изобразительных искусств имени Пушкина в Москве

Во время Троянской войны (почти 400 лет до нашей эры) разные греческие племена воевали друг с другом. Влюбился царевич Трои Парис в супругу спартанского царя Менелая Елену. И увёз её в Трою. Менелай собрал войска из Спарты и соседних городов и отправился за женой. Собственно, так началась Троянская война, которую древнегреческий писатель Гомер подробно описал в своей знаменитой «Илиаде». Долго войска Менелая осаждали Трою. А потом решили взять врага хитростью: соорудили огромного деревянного коня и оставили его у стен Трои. А сами сделали вид, что уплыли. На боку коня была прикреплена табличка с надписью: «Этот дар приносят воительнице Афине уходящие данайцы». Данайцами называло себя одно из древнегреческих племён, к которому относился Менелай.

Но трудно было обмануть троянцев, которые знали, как хитры их соседи. Жрец Лаокоон, увидев коня, воскликнул: «Что бы это ни было, а бойтесь данайцев, даже дары приносящих!» Эта фраза стала крылатой и означает, что существуют коварные подарки, которые несут гибель и горе тем, кто их получает. Лаокоон метнул в коня копьё, но отважного жреца тут же убили два огромных змея, которые выползли из моря. Так бог моря Посейдон выплеснул свой гнев на Трою.

Но Лаокоон погиб зря. Троянцы втащили красавца-коня в город, и тут же из него выскочили данайские воины, убили стражников и открыли городские ворота Менелаю.

В турецком городе Чанаккале есть деревянная статуя троянского коня, построенная для съёмок фильма «Троя». Именно на территории современной Турции располагалась в стародавние времена древнегреческая Троя.

Фото с сайта: http://travelask.ru

Письмо с вирусом может быть любым. Например, к нему мошенники прикрепят файл со ссылкой, где можно найти все рефераты, курсовые, дипломные и ещё много чего для учёбы. Только формат у файла странный. Вообще, в любом случае, когда ты по электронке получаешь письмо от незнакомого пользователя или с незнакомого адреса, лучше призвать на помощь взрослых.

Коварный «троянский конь» может поселиться в твоём гаджете и передавать твои данные мошенникам.

А при чём тут деньги, спросишь ты? Дело в том, что многие вирусы придуманы для того, чтобы вынуждать людей покупать антивирусные программы против них. Подцепил твой компьютер вирус, а следом приходит сообщение: чтобы восстановить все файлы и программы, свяжись с таким-то человеком, и он тебе за отдельную плату поможет вылечить компьютер. И ладно, если поможет, а то ведь деньги возьмёт и исчезнет. И все твои файлы просто пропадут.

Что делать?

Не открывай подозрительные файлы. Если вирус всё-таки заразил компьютер, немедленно выключи его и попроси родителей отнести его в сервисный центр. Там постараются хотя бы частично спасти данные с жёсткого диска и установят правильные антивирусные программы.

Алексей СТОПИЧЕВ

…Вот сколько интересного мы вам сегодня рассказали, ребята! И про компьютерные вирусы, и про защиту банковских карт, и даже про Древнюю Грецию! И ждём ваших работ на конкурс «ВКонтакте» с Лёвушкой».