Угрозы «цифровой» современности

Кибератаки, вымогательство и шантаж с помощью компьютерных вирусов стали одной из главных угроз «цифровой» современности. Наиболее распространенные схемы ориентированы на хищение денег у кредитно-финансовых организаций и их клиентов.

Специалисты Отделения по Орловской области Главного управления Банка России по Центральному федеральному округу рассказывают о правилах, соблюдение которых поможет не стать жертвой «цифровых» воров.

О способах, какими кибермошенники «залезают» в наши виртуальные кошельки

- Вы или ваши знакомые наверняка получали СМС с сообщением о блокировке карты, которое потом оказывалось фальшивкой. Самое удивительное то, что о такой схеме обмана знают практически все, но многие до сих пор попадаются на эту удочку. Получив такое сообщение, не паникуйте и ни в коем случае не связывайтесь с его отправителем по телефону, номер которого указан в СМС-ке. *Сразу позвоните в свой банк (номер есть на вашей карте). И вам наверняка подтвердят, что с картой все в порядке. И, разумеется, сообщите о попытке мошенничества.*
- Еще один из распространенных видов мошенничества с картами – письма с вредоносными файлами. Они приходят обычно по электронной почти или через мессенджеры, часто маскируются под «выгодные предложения» или прайс-листы. В таком письме может быть вложение либо ссылка, кликнув на которую, вы запускаете компьютерный вирус. Вредоносная программа («зловред») похищает логин и пароль онлайн-банка и отправляет их злоумышленнику. *Еще хуже, если такую ссылку вы открываете с мобильного устройства – тогда мошенники узнают и код подтверждения операции из СМС-сообщения, которое присылает банк. Тогда наверняка можете проститься с вашими деньгами.*
- Киберпреступники научились похищать данные, распространяя вредоносные плагины с более 80 тыс. сайтов в Интернете. Это зараженные программные расширения, снабжающие пользователей полезной информацией без захода на специальные сайты – курсы валют или прогноз погоды. Такие программы распространяются через магазин расширений или из непроверенных источников, они могут исполняться как в стационарных, так и в мобильных версиях браузеров. Устанавливая эти плагины, пользователь открывает злоумышленникам доступ к паролям, логинам и данным банковских карт. Ежемесячно с такими проблемами сталкиваются более 1,2 млн пользователей.

Если вы пользуетесь онлайн-банкингом, нужно заботиться не только о том, чтобы не потерять смартфон, но и всеми возможными способами защитить находящуюся в нем личную информацию

В последнее время наибольший рост числа атак фиксируется именно в сегменте мобильных платформ. А Россия оказалась лидером по количеству мобильных банковских троянов, то есть программ, предназначенных для кражи финансовой информации пользователей. В отчете компании «Лаборатории Касперского» говорится, что в прошлом году количество вредоносных установочных программ на мобильных устройствах по всему миру выросло по сравнению с 2015 годом в три раза – до 8,5 млн. *При использовании для проведения операций компьютера и мобильного телефона (все-таки это два независимых канала) информационная безопасность в известной степени обеспечивается. Если же вы совместите в одном месте и программу, и аутентификацию, и подтверждение платежа – этот порог заметно снижается.*

Самоуверенность современного пользователя часто играет на руку кибермошенникам

Сейчас в сети мошенников все больше попадают люди в возрасте до 40 лет: они очень активно пользуются гаджетами и технологиями, не сильно задумываясь о правилах. По мнению экспертов, *основными проблемами на протяжении последних четырех-пяти лет остаются: опасность заражения мобильного устройства и компьютера через интернет, недостаточность встроенных средств защиты в программные продукты со стороны разработчиков систем дистанционного банковского обслуживания, а также невыполнение пользователями элементарных требований безопасности*.

Мошенники находят причину, по которой человек легко пойдет на действия, ведущие к утрате денег.

Психологи знают, что в сфере финансов людьми в основном движут два чувства: корыстолюбие и страх. Чаще всего социальные инженеры воздействуют на желание быстро разбогатеть, получить что-то «на халяву», стремление купить что-то с большой скидкой. Очень часто давят на родственные чувства, страх за близкого человека: например, сообщают, что близкий человек якобы попал в беду.

Бóльшая часть хищений денег со счетов происходит благодаря доверчивости самой жертвы. Люди сами диктуют злоумышленникам свои пароли, номер карты, передают коды подтверждения. А этого делать категорически нельзя!

Несколько советов

Первое правило финансово грамотного человека: беречь свои персональные данные

- Ни в коем случае не реагируйте на звонки и электронные сообщения, в которых вас просят предоставить реквизиты счета, PIN-коды, пароли или персональные данные.
- Всегда используйте надежные уникальные пароли для максимально возможного количества учетных записей в интернете, а лучше всего – индивидуальный пароль для каждой из них.
- Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для «автоматического заполнения» при открытии интернет-сайта или приложения.
- Не ленитесь проверять выписки по банковским счетам и картам на предмет подозрительных транзакций.