ОРАНЖЕВЫЙ
БАНК

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

2020

УВАЖАЕМЫЕ КЛИЕНТЫ!

На фоне сложной обстановки, связанной с распространением новой коронавирусной инфекции, участились случаи мошенничества с использованием банковских карт и дистанционных систем обслуживания. Преступники применяют метод социальной инженерии, суть которого — в получении конфиденциальной информации посредством психологического воздействия на людей.

Чтобы не стать жертвой злоумышленников, пожалуйста, ознакомьтесь с распространенными сценариями, по которым они действуют, а также способами защиты от них.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ — это метод несанкционированного доступа к информации или системам ее хранения без использования технических средств.

Метод основан на манипуляции слабостями человеческого фактора и является очень эффективным. Злоумышленник получает информацию, например, путем сбора данных о конкретных объектах атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего. Преступник также может позвонить клиенту банка (под видом службы безопасности) и выведать пароль, вводя клиента в заблуждение, что с его денежными средствами пытаются совершить мошеннические действия, или сославшись на необходимость решения небольшой проблемы в компьютерной системе.

ЦЕЛЬ — получить доступ к критически важным данным (например, паспортным), учетным записям, банковским реквизитам, чтобы использовать их в дальнейшем для доступа к вашему интернет-банку и кражи денежных средств.

В любой непонятной и нестандартной ситуации, когда у вас запрашивают персональные данные и банковские реквизиты, проявляйте бдительность и осторожность, рассудительно подходите к принятию решений!

Социальная инженерия | Входящий звонок с требованием срочных действий

СИТУАЦИЯ: вам поступает звонок с информацией о том, что по вашему счету совершен несанкционированный платеж, от вас настоятельно требуют или убеждают совершить срочные действия. Возможен даже грубый разговор со стороны звонящего или, наоборот, — предложение помощи.
Главная цель злоумышленника — напугать вас, заставить в срочном порядке перевести или снять денежные средства, разгласить информацию.
У Вас определился номер банка? Не стоит доверять этому, так как мошенники научились подменять определяемые номера.

КАК СЛЕДУЕТ ПОСТУПИТЬ: если во время входящего звонка у вас запрашивают информацию, которую спрашивать не должны (кроме фамилии и даты рождения), то:

- прервите разговор и самостоятельно позвоните в банк по номеру, который указан на официальном сайте или на оборотной стороне банковской карты;

- попросите звонящего самостоятельно озвучить ответ на заданный вам вопрос, который вы подтвердите в случае его правильности.

Ни в коем случае не сообщайте злоумышленникам информацию о наличии счетов, открытых в других банках! Так злоумышленник будет сбит с толку.

НИКОГДА не верьте тому, что необходимо что-то СРОЧНО сделать.
Положите трубку и как следует все обдумайте!

Социальная инженерия | Входящий звонок — взлом системы — установка программного обеспечения для удаленного доступа

СИТУАЦИЯ: вам поступает звонок из банка, где под разными предлогами вам сообщают, что произошел, например, взлом банковской системы или банковского мобильного приложения, и для того, чтобы обеспечить безопасность счетов, необходимо сверить устройства и их операционные системы (Android и iOS), имеющие доступ к интернет банку/мобильному банку.
Для проверки злоумышленнику потребуется ваша помощь — установка программы для удаленного доступа (например, teamviewer). Такие программы позволяют постороннему человеку подключаться и совершать любые операции от вашего имени. Для этого у вас запросят ID (специальный номер) пользователя и пароль, сообщив которые, злоумышленник сможет легко подключиться и завладеть конфиденциальной информацией смартфона.

КАК СЛЕДУЕТ ПОСТУПИТЬ: прервите разговор и самостоятельно позвоните в банк по номеру, который указан на официальном сайте или на оборотной стороне банковской карты, и уточните ситуацию, озвученную во входящем телефонном звонке.

НИКОГДА не устанавливайте программы на компьютер и смартфон под диктовку.

Социальная инженерия | Входящий звонок — перевод на автоматическую линию

СИТУАЦИЯ: вам поступает звонок из банка, где под разными предлогами для «спасения» денежных средств/разблокировки банковского счета или карты вас переводят в автоматическую систему, где запрашиваются все данные по карте.

Тут главное — понимать, что автоматическое меню — поддельное, и это до сих пор входящий вызов, который вы не инициировали.

КАК СЛЕДУЕТ ПОСТУПИТЬ: не вводите персональную и банковскую информацию!

- Прервите разговор и самостоятельно позвоните в банк по номеру, который указан на официальном сайте или на оборотной стороне банковской карты, чтобы прояснить ситуацию.

- Во время входящего звонка при переводе в голосовое меню не вводите персональную информацию.

Социальная инженерия | Входящий звонок — потенциальный покупатель

СИТУАЦИЯ: мошенничество на торговых интернет-площадках. Вам звонят, спрашивают о товаре, который вы продаете. Затем говорят, что хотят оплатить прямо сейчас всю сумму, чтобы забронировать за собой этот товар. И для этого просят информацию о банковской карте. Но запрашивают не только номер карты, а полностью все сведения о ней, в том числе и код на обратной стороне.

Через небольшой промежуток времени вам могут перезвонить и попросить сделать выписку по движению денежных средств через онлайн-банк, предлагая свою помощь. Когда вы соглашаетесь, вам диктуют, что необходимо делать, забалтывают, и вы, не осознавая этого, разглашаете свои логин, статичный пароль, одноразовыйпароль из СМС.

КАК СЛЕДУЕТ ПОСТУПИТЬ: назвать можно ТОЛЬКО НОМЕР КАРТЫ для осуществления перевода.

НИКОГДА не совершайте никакие ДЕНЕЖНЫЕ переводы под диктовку.

Социальная инженерия | Фишинг

СИТУАЦИЯ: вам на электронную почту поступило письмо о том, что вы выиграли в акции/розыгрыше призов, и для получения выигрыша необходимо пройти по ссылке и заполнить анкету.

Такой вид мошенничества называется фишингом, он базируется на незнании пользователями основ сетевой безопасности. В частности, многие не в курсе простого факта — сервисы не рассылают письма с просьбами сообщить свои учетные данные, пароль и прочее.

КАК СЛЕДУЕТ ПОСТУПИТЬ: если вам пришло письмо о выигрыше с вложениями или ссылками, а вы ни в каком розыгрыше не принимали участие, то необходимо пожаловаться на СПАМ и удалить письмо, не открывая вложения и ссылки в нем.

Социальная инженерия | Актуальные схемы мошенничества на фоне распространения коронавирусной инфекции

СИТУАЦИЯ: злоумышленники используют методы социальной инженерии, рассылая приманки в связи с ситуацией в мире, вызванной коронавирусной инфекцией, на электронную почту, через текстовые сообщения в мессенджерах и социальных сетях, а также используя телефонные звонки:

1. Вам на электронную почту поступает письмо о том, что вам положена компенсация/субсидия от государства и для ее получения необходимо перейти по ссылке и заполнить анкету, где необходимо ввести реквизиты банковской карты.
2. Вам на мобильный телефон в один из мессенджеров приходит приглашение якобы от имени единого портала Госуслуг с темой «Важная новость» и текстом «Получите компенсацию за карантин».
3. В социальных сетях увеличилось количество поддельных групп и пользователей, распространяющих заведомо ложную информацию с указанием фишинговых ссылок (проверка по данным банковской карты, где можно перемещаться по городу; предложение улучшить рейтинг платежеспособности в кредитной истории и т.д. и т.п.).
4. Телефонные мошенники представляются сотрудниками медицинских организаций, Роспотребнадзора и других ведомств. Предлагают переводить им средства за экспресс-тесты на коронавирус, медицинские препараты и т.д.

КАК СЛЕДУЕТ ПОСТУПИТЬ: необходимо проявлять внимание и бдительность, с подозрением относиться к любому текстовому сообщению, электронному письму или телефонному звонку, где запрашивают информацию о ваших персональных данных, данные банковских карт и т.п., и не переходить по подозрительным ссылкам.

ОРАНЖЕВЫЙ
БАНК

БЛАГОДАРИМ ЗА ВНИМАНИЕ!

СВЯЗАТЬСЯ С НАМИ

Тел.: 8 800 500 80 88
E-mail: client@bankorange.ru
Skype: BankOrange
Viber: +7 921 765 69 54
WhatsApp: +7 921 765 69 54