ВЗЛОМ МОЗГА

КАК МОШЕННИКИ УБЕЖДАЮТ ОТДАВАТЬ ИМ ДЕНЬГИ

На смену традиционным ограблениям со взломом приходят хищения электронных денежных средств, причем жертва сама добровольно дает бандитам доступ к своему онлайн-банку или же переводит деньги на нужный счет. Приемы, побуждающие граждан действовать по сценарию злоумышленников, относятся к социальной инженерии, и ее эксперты по кибербезопасности называют главной проблемой настоящего времени.

Социальную инженерию иногда называют наукой и искусством взлома человеческого сознания. Используя ее, мошенники имеют своей целью выманивание конфиденциальной информации у жертв либо побуждают жертв к совершению действий, направленных на проникновение в систему в обход системы безопасности. В результате атак с использованием социальной инженерии теряют деньги не только граждане, но и компании и банки.

Банк России называл социальную инженерию одной из главных проблем в информационной безопасности в 2017 году. С ним согласны эксперты. «Злоумышленники все больше уходят в область психологии, выделяя для себя профили по вероятности попадания различных социальных групп граждан под воздействие методов социальной инженерии и выбирая наиболее эффективные из них, то есть целевую группу, назовем ее „модель жертвы“»,— констатирует руководитель направления консалтинга ГК InfoWatch Мария Воронова.

Рассмотрим основные «модели жертв», на которые ориентируются злоумышленники.

Продвинутый средний класс

Трендом 2017 года эксперты по информбезопасности называют атаки злоумышленников, направленные на молодых людей в возрасте 26–40 лет, относящихся к среднему классу.

Данная целевая группа имеет два несомненных преимущества. Первое — это достаточно обеспеченные и занятые люди, которые не будут из-за потери нескольких сотен (а порой и тысяч) рублей обращаться в полицию. Значит, злоумышленники могут не опасаться уголовной ответственности. Второй плюс — люди из данной целевой группы много времени проводят в соцсетях, где весьма охотно рассказывают друзьям о совершенных на них атаках. Мошенникам достаточно анализировать сообщения в сетях, чтобы выявить работающие методы и копировать их. «Преступники в принципе не склонны к импровизации, действуют по проверенным сценариям, которые подтверждены опытом их коллег»,— предостерегают в InfoWatch.

Однако людей из этой целевой группы нельзя назвать легковерными, потому мошенники при атаке на данную категорию граждан могут использовать информацию, полученную при анализе тех же профилей в соцсетях или же из купленных на черном рынке баз данных. «Например, при звонке злоумышленники обращаются к жертве по имени-отчеству, и это может создать ощущение, что на том конце провода человек знает, с кем говорит,— рассказывает заместитель главы ГуБЗИ ЦБ Артем Сычев.— При этом на самом деле злоумышленники совершенно точно не знают, с кем общаются». Также злоумышленники могут знать дату рождения человека, место работы и т. д.

Чаще всего в данном случае злоумышленники представляются сотрудниками банка. «Например, подавшим заявку на кредит звонит якобы менеджер банка и сообщает, что заявка на кредит одобрена, просит предоставить реквизиты банковской карты для зачисления средств,— рассказывает Артем Сычев.— В итоге вместо зачисления денег происходит списание». Вариант подобной схемы — когда «сотрудник банка» сообщает, что у кредитной организации нет офиса в данном городе, и просит направить небольшую сумму комиссии за перевод средств из города в город, рассказал господин Сычев.

По словам экспертов, часто звонят под видом менеджера Сбербанка, поскольку с большой долей вероятности у клиента будет карта именно этого банка.

Наиболее популярные варианты хищения — это побуждение жертвы перевести средства куда-либо или же дать доступ к онлайн-банку.

Доверчивые пенсионеры

Доверчивостью лиц преклонного возраста традиционно пользуются все мошенники, применяющие социальную инженерию. Эта категория граждан наиболее доверяет официальным учреждениям — налоговой службе, Пенсионному фонду и т. д., и потому часто звонки поступают от их имени.

Например, в 2017 году широко использовалась легенда, когда злоумышленники звонили под видом сотрудников ЦБ и предлагали компенсации детям войны. «Несколько лет назад данная легенда уже использовалась, потом она была совершенно забыта и в 2017 году начала активно использоваться снова»,— отметил Артем Сычев.

Клиент с вопросами

Банковский клиент, который пытается что-либо выяснить на странице кредитной организации в соцсетях, также рискует стать жертвой мошенников. Как подсчитали аналитики Group-IB, количество злоумышленников, под видом сотрудников банков вымогавших персональные данные в соцсетях, в 2017 году выросло вдвое. Схема мошенничества такова — пользователь публикует на страничке банка в соцсетях вопрос или иное сообщение. Например, хочет уточнить условия получения кредита. Или оставляет жалобу на того или иного сотрудника. Традиционно реальный сотрудник кредитной организации отвечает в течение нескольких часов. Мошенники же реагируют куда более оперативно. Буквально через несколько минут оставившему сообщение клиенту может прийти личное сообщение якобы от представителя кредитной организации. Предлагая помочь решить проблему, он пытается получить доступ к онлайн-банкингу клиента. Например, для повышения уровня доверия может инициировать отправку на мобильный телефон клиента одноразового пароля — для этого нужен лишь логин для входа в личный кабинет. По статистике, чаще всего злоумышленники действуют в сети «ВКонтакте».

Любители халявы

Уж сколько раз твердили миру, тем не менее и среди молодежи, и среди представителей вполне зрелого возраста нередко встречаются люди, которые верят в неожиданно свалившуюся на них удачу. Если такая вера подкреплена низкой финансовой грамотностью и незнанием технологий, то они — точно в зоне риска.

Примером подобной схемы является хищение средств с использованием платежных терминалов Сбербанка. Например, человеку приходит СМС о том, что Сбербанк предлагает своим клиентам (а это идет массовая рассылка сооб-

ТЕКСТ **Вероника Никитина**
ФОТО **Евгений Павленко**