Министерство образования и науки Российской Федерации
ФГБОУ ВО «Арктический государственный агротехнологический университет»
Колледж технологий и управления
38.02.01 «Экономика и бухгалтерский учет (по отраслям)»

Эссе
по «Кибербрифингам»
на тему: «Как безопасно совершать онлайн-покупки»

Выполнил:
студент первого курса
группы БУ-11-22
Захаров А.В.

Якутск 2022 г.

Предлагаю мысленно перенестись на 20 лет назад, когда чтобы совершить покупку необходимо было сделать определенный алгоритм действий: выбрать день похода за покупками, так как это могло отнять целый день, определиться что и за чем нужно приобрести, чтобы зря времени не терять и наконец поехать за покупками. Удивительно, что всего через несколько лет появится возможность приобретать товары для обыденного пользования от хозтоваров и продуктов до электроники и бытовой техники не выходя из дома. Но с удобством пришел и риск быть обманутым, если раньше при походе за покупками основной риск представляли воровство и недодача сдачи, то теперь все это вышло на новый, более продвинутый уровень. Под риском не только сдача и товар, но и все сбережения, которые хранятся на счетах в банках. И на данной работе разберемся как обезопасить себя и свои доходы от мошенников.

Если рассматривать тенденции на сегодняшний день атакам кибермошенников подвергается преимущественно экономически активное население в возрасте 20-60 лет (69%). «Яндекс.Маркет» и компания GfK Rus исследовали российскую аудиторию интернет-магазинов и выяснили, что каждый второй житель страны в возрасте 16−55 лет покупает что-нибудь в интернете хотя бы два раза в год. Из этого следует, что потенциальные жертвы кибермошенников исчисляются сотнями тысяч людей. И чтобы избежать этого необходимо понять, как работают кибермошенники, ведь это далеко не «хакерские» навыки, которые мы привыкли видеть в фильмах, здесь большую роль играет «социальная инженерия». *Социальная инженерия (social engineering)* или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию. Это первое что надо понять самое уязвимое место не банк, не кредитная или дебетовая карта, а человек, то есть Вы. Здесь как раз подойдет именитая пословица «Предупрежден - значит вооружен», зная, что целью атаки являетесь именно Вы, вам легче будет предотвратить наихудший сценарий.

Каждый раз совершая покупку-онлайн в большинство случаев

приходиться вводить информацию о карте: 16 цифр на лицевой части, срок действия, CVC-код и имя держателя карты. И как бы страшно и опасно это не выглядело большинство банков предусмотрело двухфакторную аутентификацию посредством СМС-кода или же PUSH-уведомления от приложения. Что практически сводит к нулю попытку совершить покупку без Вашего ведома, если только смартфон вместе с СИМ-картой не находятся у злоумышленника.

И тут возникает вопрос, что тогда злоумышленнику необходимо сделать, чтобы украсть ваши денежные средства с карты. Во-первых узнать данные Вашей карты, например, если Вы совершаете покупки или вводите данные о своей карте на подозрительных сайтах, заходите на проверенные сайты через стороннюю ссылку, либо зашли на сайт на котором часто совершаете покупки, но не проверили URL сайта (вместо: https://www.wildberries.ru/, может быть https://www.wildberies.ru/. https://www.wildberris.ru/ и т.д и т.п.) согласитесь, что опечатки минимальны и их можно и не заметить. И вот когда злоумышленник получил Ваши данные, ему необходимо получить от Вас заветный СМС-код или PUSH-уведомление. И тут вступает в дело «социальная инженерия», злоумышленнику необходимо связаться с Вами, один из самых распространенных способов это телефонный звонок. Посредством звонка злоумышленники в основном представляются Службой безопасности банка в котором выпущена Ваша карта. И уверенным, множество раз отрепетированной фразой начинают наступление: «Добрый день это СБ Вашего банка... была выявлена попытка подозрительной транзакции... сообщите нам код из СМС для предотвращения операции...». Можете быть уверены, что настоящего профессионала практически нельзя уличить во лжи, ведь они буду обращаться к Вам по имени и отчеству, будут знать последние операции по Вашим картам и даже в некоторых случаях им будет известен баланс на карте, они сделают все чтобы им поверили. И тут надо помнить, что насколько бы убедительными не звучали их слова не надо поддаваться панике и совершать необдуманные действия. На самом деле все гораздо проще после звонка кибермошенника не предпринимая какие-либо действия необходимо связаться с Вашим банком по

горячей линии и узнать действительно ли были попытки транзакции о котором говорил злоумышленник. Если нет, то желательно карту заблокировать и перевыпустить новую. На этом вы предотвратили попытку обмануть Вас. Но если все же Вы поддались панике и пошли на поводу злоумышленника. Обязательно нужно выполнить ряд мероприятий:

- Первое действие после того, как вы недосчитались на своем банковском счете некоторой суммы, – это отключить смартфон и вытащить из него СИМ-карту. Это потенциальное орудие киберпреступления, так что нужно обеспечить его сохранность для сотрудников правоохраниельных органов. Самое глупое, что можно сделать в этой ситуации, - отдать устройство в сервисную службу.
- Второе действие - как можно скорее связаться с банком и отозвать денежный перевод, а заодно блокировать все возможные действия с расчетным счетом.
- Шаг третий – написать заявления в двух экземплярах. Предоставить заявления в банк необходимо в течение одного дня с момента атаки кибермошенников.
- Шаг четвертый - получить в банке детализацию с расчетного счета и обратиться в банк, в который ушли деньги по инициативе злоумышленника
- И наконец, третье заявление - о факте хищения денежных средств - необходимо предъявить в полицию. Для оформления дела понадобится документальное подтверждение хищения денежных средств: выписка из банка, детализация расходов и т. д.

Ведь любую проблему можно решить даже, если стали жертвой не стоит отчаиваться. В наше время борьба с киберпреступностью является одной из приоритетных целей государства.

Если Вы все же активный пользователь онлайн-покупок, лучшим решением будет завести дополнительную карту только для онлайн-оплат. Где будут находиться денежные средства ровно в том количестве сколько необходимо для оплаты покупки.

В заключении обязательно надо упомянуть, что именно Вы являетесь тем звеном, который связывает Ваши денежные средства и злоумышленника. Будьте осторожны и не поддавайтесь на провокации и убеждения без достоверной базы.

В данной работе были перечислены далеко не все способы кражи и социальной инженерии, но суть всегда одна: это манипуляция людьми для достижения своих целей у злоумышленника, и максимальная осторожность и уверенность в своих действиях со стороны жертв. Наш мир вступил в эру информационных технологии, где безопасность и конфиденциальность базы данных всегда будут обновляться и улучшаться, как и способы краж и взлома этих данных, и слабым звеном в этой сфере всегда будет человеческий фактор и сам человек.