Тема 6: Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Социальная инженерия используется ежедневно обычными людьми в повседневных ситуациях. Например, во взаимодействии педагогов со своими учениками. Врачи, психологи и психотерапевты часто используют элементы социальной инженерии, чтобы “манипулировать” своими пациентами, для принятия мер, которые помогут пациенту, а мошенник использует элементы социальной инженерии, чтобы убедить его выполнить действия, необходимые злоумышленнику или раскрыть информацию. Хотя конец игры сильно отличается, подход может быть очень похож. Психолог может использовать ряд хорошо продуманных вопросов, чтобы помочь пациенту прийти к выводу, что необходимы перемены. Аналогичным образом мошенник будет использовать ряд хорошо продуманных вопросов, чтобы поставить его цель в уязвимое положение. Как и любой инструмент, социальная инженерия не является «хорошей» или «плохой», это просто инструмент, который имеет много различных применений.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляции людей, которые приводят к совершению действия или разглашению конфиденциальной информации. Это может быть злоупотребление доверием с целью сбора информации. Социальная инженерия часто является одним из многих шагов в более сложную схему мошенничества.

В общем значении социальная инженерия - это акт манипуляции человеком, который провоцирует выполнить действие, которое как может быть в интересах человека, так и в интересах злоумышленника.

Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на

незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Целью фишеров сегодня являются клиенты банков и электронных платёжных систем. Часть последних фишинговых атак была направлена непосредственно на руководителей и иных людей, занимающих высокие посты в компаниях.

Социальные сети также представляют большой интерес для фишеров, позволяя собирать личные данные пользователей: в 2006 году компьютерный червь разместил на MySpace множество ссылок на фишинговые сайты, нацеленные на кражу регистрационных данных; в мае 2008 года первый подобный червь распространился и в популярной российской сети ВКонтакте. По оценкам специалистов, более 70 % фишинговых атак в социальных сетях успешны.

Человек всегда реагирует на значимые для него события. Поэтому фишеры стараются своими действиями встревожить пользователя и вызвать его немедленную реакцию. Поэтому, к примеру, электронное письмо с заголовком «чтобы восстановить доступ к своему банковскому счёту …», как правило, привлекает внимание и заставляет человека пройти по веб-ссылке для получения более подробной информации.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками.

Фишеры часто вместо текста используют изображения, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами. Но специалисты научились бороться и с этим видом фишинга. Так, фильтры почтовых программ могут автоматически блокировать изображения, присланные с адресов, не входящих в адресную книгу. К тому же появились технологии, способные обрабатывать и сравнивать изображения с сигнатурами однотипных картинок, используемых для спама и фишинга.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием

настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё (от веб-адреса до сертификатов) выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков.

Для противостояния антифишинговым сканерам фишеры начали использовать веб-сайты, основанные на технологии Flash. Внешне подобный сайт выглядит как настоящий, но текст скрыт в мультимедийных объектах.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счёта и PIN-код. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. Чаще всего злоумышленники выдают себя за сотрудников службы безопасности банка и сообщают жертве о зафиксированной попытке незаконного списания средств с его счёта. В конечном счёте, человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг. Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем».

Существуют различные методы для борьбы с фишингом, включая законодательные меры и специальные технологии, созданные для защиты от фишинга.

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) специалисты советуют связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, эксперты рекомендуют самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном

сообщении.

Детская пластиковая карта

В банках всё чаще стали появляться предложения для детей и подростков, направленные на отказ от налички. Это не только специальные карты, но и приложения для бесконтактной оплаты. Всё бы ничего, но есть у этих платёжных карт подвох — кешбэк, как у взрослых.

Безналичная оплата всё активнее развивается в нашей стране: количество операций по безналичной оплате картами уже приближается к 80% от всех карточных транзакций. И вполне естественно, что этот тренд дошёл и до детских карманных расходов.

Открыть счёт ребёнку можно по достижении им 14-летия и с письменного согласия родителей.

Зачем банкам несовершеннолетние клиенты?

Выпуская на рынок этот новый продукт, банки обеспечивают себя постоянным наличием лояльных клиентов: дети вырастают и продолжают пользоваться услугами банка.

— Чтобы привлечь клиентов к открытию детских карт, разрабатываются условия, призванные обеспечить безопасность и удобство их использования: это и яркий дизайн, и низкая стоимость годового обслуживания, и возможность установить дневной или месячный лимит расходов или запрет на использование детской карты для снятия наличных в банкомате, перевода денег на другие карты или покупок в Интернете.

К плюсам детских банковских карт можно отнести и то, что с их помощью родители получают возможность легко контролировать траты своих детей. И этот контроль намного эффективней, чем в случае с наличными. Родитель получает СМС о каждой операции ребёнка, так что может видеть, на что именно были потрачены деньги. Кроме того, все траты обычно видны в банковском приложении или в интернет-банке. Родитель видит также, сколько денег на данный момент доступно ребёнку, в случае необходимости можно всегда пополнить карту в режиме онлайн.

Оптимальный вариант, когда банк, выпуская детскую карту, привязывает её к отдельному счёту, а не к основному счёту родителя. Во-первых, это безопаснее: на отдельный счёт ребёнка родитель переводит небольшие суммы на карманные расходы, в случае утери детской карты нет риска, что мошенники воспользуются средствами на "взрослом" счёте. Во-вторых, так проще контролировать "детский" остаток. Безусловно, никакой банк не откроет счёт ребёнку в 7 лет. "Детский" счёт по факту открывается на имя родителя, но ребёнок получает к нему доступ с помощью своей карты.

С помощью банковской карты дети научатся в будущем контролировать

финансовые расходы.

Опасности при использовании детской пластиковой карты такие же, как и у взрослых. Нужно заранее рассказать о мошенниках, объяснить, что нельзя никому называть данные карты, иначе есть риск потерять деньги с родительского счёта.

Необходтмо родителям отнестись к выбору такого продукта очень внимательно.

Обычно банки выпускают детям карты при условии, что родитель также оформляет взрослую карту в этом банке. Нужно ознакомиться с тарифами, годовое обслуживание взрослой карты может быть уже не бесплатным. Кроме того, взрослая карта может предполагать кредитный лимит. Необходимо выяснить, какой процент банк взимает по кредитной карте, какова продолжительность льготного периода, какие предлагаются бонусные программы. Нужно учитывать, что бесплатность детской карты банк может компенсировать финансовыми продуктами для родителей. Естественно, банку в этом случае выгодно, чтобы родитель пользовался кредитным лимитом, не укладывался в льготный период и платил банку проценты за пользование деньгами.

При грамотном подходе и правильном выборе банка детская кредитка — удобный продукт как для ребёнка, так и для родителя, даже если ему тоже придётся оформить карту этой кредитной организации.

Деньгами на этом банковском счёте/карте подросток может распоряжаться самостоятельно:

- снимать наличные;
- переводить деньги на карты другим людям;
- получать переводы от частных лиц;
- оплачивать покупки и услуги в розничных точках или через интернет;
- пополнять телефон, в т.ч. другим лицам;
- управлять операциями и контролировать баланс карты в мобильном .

Вопрос родительского контроля за молодежной картой законодательно не урегулирован. Банки по собственному усмотрению решают этот вопрос в правилах выпуска карт. Это значит, что банк может отказать родителям в предоставлении возможности контроля за операциями по карте подростка. Или дать согласие, при условии оплаты данной услуги.

Чтобы уберечь ребенка от необдуманных трат родители могут:

- Настраивать лимиты на покупки, снятие денег с карты.
- Отключить возможность расплачиваться дополнительной картой в интернете. При каждой попытке ребенка совершить онлайн-покупку родителю будет приходить СМС с кодом подтверждения операции.

- Запретить снимать с карты наличные, переводить деньги на другие банковские карты или счета.
- Получать отчеты обо всех операциях, совершаемых по карте.
- Отслеживать баланс карты.
- Просматривать историю операций.
- Заблокировать карту.

Как защитить банковскую карту ребенка от мошенников

Перед тем, как ребенок начнет пользоваться банковской картой установите на телефон ребенку лицензионную антивирусную программу. И расскажите ему об основных правилах финансовой безопасности:

Объясните, что на банковской карте указаны персональные данные: фамилия и имя держателя, срок действия карты, CVV-код, которые нельзя никому сообщать.

Нельзя фотографировать карту, хранить фото карты в телефоне, делиться им в соцсетях и мессенджерах.

Никому не сообщать ПИН-код карты, а также секретные коды, которые приходят в СМС-сообщениях на телефон для подтверждения покупок.

Прикрывать рукой клавиатуру при наборе ПИН-кода в банкомате или платежном терминале.

Помогите ребенку выучить наизусть ПИН-код от карты. Расскажите, почему нельзя записывать ПИН-код на карте, хранить его вместе с картой в кошельке.

Никому не давать свою банковскую карту, включая одноклассников, друзей.

При утере детской карты срочно сообщить об этом родителям, молодежной карты – позвонить в банк по телефону «горячей» линии.

Не совершать покупки в интернете и не вводить никаких персональных данных на незнакомых и подозрительных сайтах. Если есть хоть малейшие сомнения в надежность сайта – советуйся с родителями.

Не совершать покупки при входе в интернет в общественных местах через незапароленные точки Wi-Fi.

Не переходить по ссылкам из смс сообщений и из писем в формате HTML, особенно с незнакомых телефонных номеров и электронных адресов.

Скачивать понравившиеся приложения, игры и т.п. только из официальных магазинов приложений.

Подводя итоги

При грамотном подходе и правильном выборе банка детская карта — удобный финансовый инструмент как для ребёнка, так и для родителя.

Перед началом пользования картой, объясните ребенку базовые правила безопасного пользования картой. Не критикуйте покупки ребенка, даже если считаете, что он тратит деньги на ерунду.

Это его деньги, дайте ребенку право на ошибки и получение собственного финансового опыта. А вы, как родители, ненавязчиво обсуждайте с детьми последствия различных трат, подсказывайте, что можно сделать лучше. Так ребенок быстрее научится грамотно распоряжаться деньгами и будет видеть в вашем лице союзника, а не сурового критика.