kaspersky

Социальная инженерия

Методические рекомендации для учителя

kaspersky

Социальная инженерия

Методический материал носит рекомендательный характер, и учитель, принимая во внимание особенности класса, может изменять вопросы и дополнять задания.

Цель урока:

Сформировать знания и умения у учащихся о понятии социальной инженерии и ее основных методах, рассмотреть конкретные примеры их использования мошенниками и разработать правильный ответный алгоритм действий на такие угрозы.

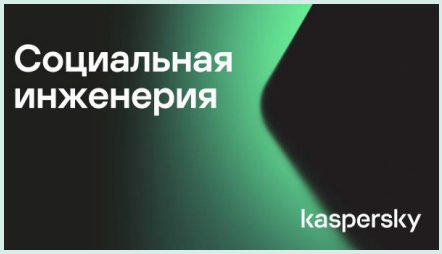
Ключевые слова:

- **Социальная инженерия**
- **Мошенники**
- **Фишинг**
- **Претекстинг**
- **Социальные сети**
- **Вредоносное ПО**

Методическое обеспечение и средства обучения:

- **Презентация**
- **Материал для учителя**
- **Рабочий лист ученика**

Таблица 1. Комментарии к каждому слайду

Слайд	Комментарии
	После приветственных слов и обозначения темы мероприятия следует провести опрос: • Знакомы ли учащиеся с понятием «социальная инженерия»? • Получали ли они или их близкие нежелательные звонки, SMS, сообщения в социальных сетях, авторы которых пытались получить ответную реакцию? • Какое ПО учащиеся и их родители используют для защиты своего личного информационного пространства? • Какие знания психологии человека могут быть использованы мошенниками во вред? После проведения дискуссии приходим к выводам, что рассмотренные ситуации связаны с психологией человека, при этом используются продвинутые информационные технологии. Поэтому понятие «социальная инженерия» рассматривается в контексте информационной безопасности.

Социальная инженерия подразумевает манипуляции действиями человека без использования технических средств. В контексте кибербезопасности – незаметное принуждение пользователя сделать что-то, что подвергает риску его безопасность или безопасность организации, в которой он работает.

Успех в значительной степени зависит от удачной маскировки вредоносных и нежелательных сообщений под легитимные (в некоторых могут быть даже советы по борьбе с киберпреступностью).

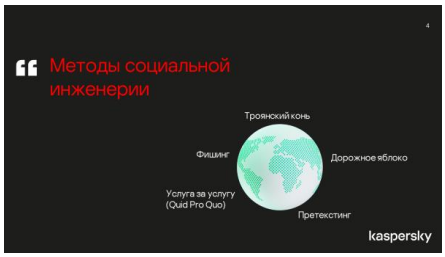
Цель – вызвать ответную реакцию у жертвы: щелкнуть по зараженному вложению электронной почты, перейти по вредоносной ссылке или ответить на ложное уведомление.

После формулировки цели социальной инженерии, по каждому отдельному пункту приводим примеры, выслушиваем примеры учащихся.

Примеры:

- Загрузка установочного файла из сообщения, полученного на электронную почту.
- Получение в мессенджере сообщения от друга с ссылкой на сайт для голосования.
- Ведение разговора с абонентом, чей телефонный номер поддельный и совпадает с телефонным номером известного банка.

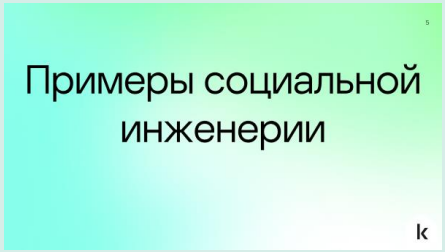
Распространенные методы социальной инженерии:



- **Услуга за услугу** – метод выполняется мошенниками, которые не имеют в своём арсенале продвинутых инструментов взлома, однако проводят предварительное исследование целей. Используя этот метод, злоумышленники под видом доброжелателей стимулируют жертву сделать определенные действия для них, что в скором времени приведет к колоссальной личной выгоде.
- **Фишинг** – метод нацелен на кражу конфиденциальной информации, такой как учетные данные от аккаунтов в интернет-сервисах или данные банковских карт. Типичная фишинговая атака состоит из рассылки писем или сообщений от имени легитимных организаций с темой-«приманкой» и ссылкой на поддельную страницу ввода данных, а также рассылка писем или сообщений со ссылками на страницы загрузки вредоносного ПО или с вредоносными вложениями.
- **Троянский конь** – метод получил название в честь мифа, так как жертва сталкивается с подменой необходимого объекта на какой-либо вредоносный, внешне никак это не проявляющий. Примером может служить скачивание установочного файла на компьютер не с официального источника и дальнейшую установку приложения. Но после завершения данного процесса жертва столкнется с тем, что компьютер работает неисправно, либо требует

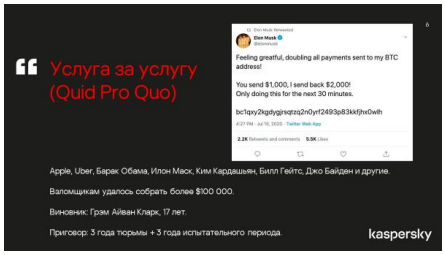
определенных манипуляций, которые вынуждают делать мошенники.

- **Дорожное яблоко** – метод состоит в адаптации предыдущего метода и требует обязательного применения какого-либо физического носителя информации (флешки или диски, которые стилизованы логотипами известных компаний, либо имеют надписи с «интересными» для жертвы словами). Такой носитель информации размещают на пути жертвы, например, рядом с машиной на парковке, на кратчайшем пути от остановки общественного транспорта до офиса, на рабочем столе т.д., чтобы при обнаружении возник интерес проверить, что находится на носителе.
- **Претекстинг** – метод включает в себя некое действие, отработанное по заранее составленному сценарию (претексту). В результате жертва должна выдать определённую информацию или совершить определённое действие. Метод чаще всего используется в телефонном разговоре. Включает в себя больше, чем просто ложь, и требует какого-либо предварительного поиска информации для ее персонализации, чтобы обеспечить доверие у жертвы.



После введения определения социальной инженерии и рассмотрения распространённых методов переходим к конкретным примерам по каждому случаю.

Услуга за услугу.



История произошла 15 июля 2020 года.

Большое количество Twitter-аккаунтов стали распространять однотипные сообщения: «Все биткойны, отправленные на указанный внизу адрес, вернутся в удвоенном количестве! Если пошлете $1000, я верну вам $2000. Делаю это только следующие 30 минут».

Эти сообщения рассылались от имени известных людей и крупнейших компаний. Классический биткойн-развод, и в этом не было бы ничего интересного, если бы не один важный нюанс: все эти аккаунты были настоящими – они действительно принадлежали известным людям и крупнейшим компаниям.

Сначала мошеннические сообщения стали появляться в Twitter-аккаунтах, напрямую связанных с криптовалютами: раздачу анонсировали основатель криптобиржи Binance Чанпэн Чжао, страницы нескольких других криптобирж, включая Coinbase, и тематический новостной сайт Coindesk.

Но этим дело не ограничилось, один за другим к этой мошеннической схеме стали присоединяться новые и новые аккаунты, принадлежащие бизнесменам, знаменитостям, политикам и компаниям: Apple, Uber, Бараку Обаме, Илону Маску, Ким Кардашьян, Биллу Гейтсу, Джо Байдену (который на тот момент еще не был президентом США), Джеффу Безосу, Канье Весту и так далее.

За те несколько часов, пока в Twitter искали корень проблемы, взломщикам удалось собрать более $100 000 – сумма немалая, но, конечно же, не идущая ни в какое сравнение с ударом по репутации социальной сети.

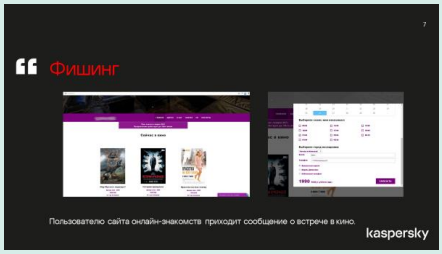
Довольно быстро выяснилось – хакерам удалось получить доступ к внутренней системе Twitter для управления аккаунтами, причем первоначально предполагалось, что в этом им помог некий инсайдер.

Однако на деле все оказалось иначе. Хакеров довольно быстро удалось найти и арестовать, причем руководителем коллектива взломщиков оказался американский школьник – семнадцатилетний (на момент взлома) Грэм Айван Кларк.

В итоге он получил 3 года тюрьмы и еще 3 года испытательного периода. Но главное, в процессе расследования удалось выяснить, что хакеры обошлись без помощи инсайдера. Вместо этого они использовали социальную инженерию и фишинг, чтобы получить доступ к системе от сотрудников Twitter.

Для начала они провели исследование в LinkedIn (американская социальная сеть для поиска и установления деловых контактов), с помощью которого выявили сотрудников, вероятно, имеющих доступ к системе управления учетными записями. После этого с помощью функции LinkedIn для рекрутеров они добыли контактную информацию этих сотрудников, включая номера сотовых телефонов. Далее они звонили работникам Twitter, представлялись коллегами и при помощи ранее собранных данных убеждали тех посетить фишинговый сайт, имитирующий страницу входа во внутренние системы Twitter.

Таким образом они заполучили пароли и коды двухфакторной аутентификации, с которыми смогли в итоге войти в систему управления учетными записями Twitter и завладеть десятками аккаунтов с миллионами подписчиков.



Фишинг.

Схема, о которой пойдет речь, связана с частными кинозалами. Начинается все с того, что пользователю, разместившему анкету на сайте онлайн-знакомств, в один прекрасный день приходит сообщение от красивой девушки.

Фальшивый аккаунт формируется за счет фотографий реального человека, который размещает их в своих социальных сетях, не

задумываясь и не зная, что их используют мошенники в своих целях.

После непродолжительного общения диалог подразумевает встречу в реальной жизни. Куда же сходить на первое свидание? Разумеется, в кино – такое предложение поступает с поддельного аккаунта.

Но предлагается сходить не в обычный кинотеатр, а в «как будто сделанный для вас двоих» – в частный кинозал, где кроме вас никого больше не будет. И присылает ссылку на сервис по бронированию билетов.

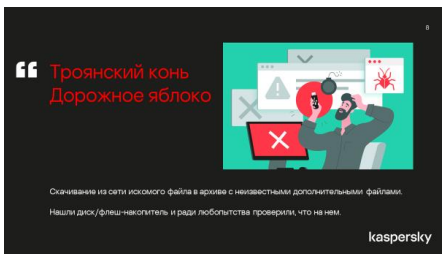
После выбора подходящего сеанса и ввода необходимой информации сайт перенаправляет на страницу оплаты. После этого у мошенников есть все данные банковской карты.

Следует отметить, что часто, при подделывании сайтов, мошенники формируют не весь его функционал, а только нужные страницы. В примере про кинотеатр сайт был полностью рабочим, с работающей службой поддержки, с указанием адресов в разных городах страны, при проверке которых через карты становилось ясно, что это какой-либо торговый центр с зоной развлечений.

Что могло выдать, что это фишинговый сайт?

- Графа «Счет получателя» при онлайн-оплате: в ней написано, что перевод отправится физическому лицу, но раздел с контактами на сайте утверждает, что владелец сети кинозалов – компания, то есть лицо юридическое.
- ИНН организации в разделе «Контакты»: при его проверке на сайте Федеральной налоговой службы получаем, что организация с таким ИНН имеет другое название и занимается другим направлением.
- Домен сайта: при проверке даты регистрации домена и его владельца через сервис WHOIS выяснилось, что его зарегистрировали на частное лицо, а не на организацию, и произошло это всего несколько недель назад, что является очень подозрительным.

Троянский конь и дорожное яблоко.



Рассматриваем два данных метода совместно, так как зачастую они используются одновременно.

Говоря о троянском коне, можно привести пример загрузки файла установщика из непроверенного источника.

В основном это какой-либо установочный файл с вредоносным содержимым, которое маскируется под видом востребованного приложения или программы.

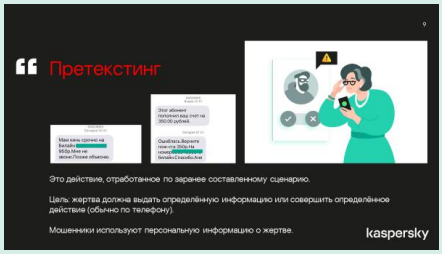
В большинстве случаев такие файлы маскируют под видом архивов, чтобы ввести в заблуждение пользователя. Процесс установки вредоносного ПО выглядит как его распаковка.

Примером для метода дорожного яблока может служить анализ мошенниками мест расположения конкретных компаний и возможные наикратчайшие пути следования от ближайших остановок общественного транспорта до данной организации. Так как ими пользуются многие сотрудники, то в таких местах они

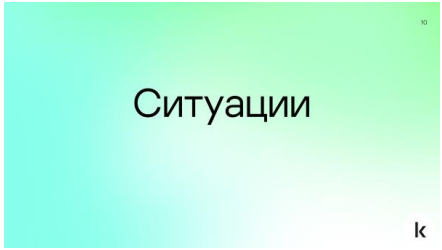
будут находить флеш-накопители с лейблом компании, либо интересной подписью владельца. Что только привлечет интерес к проверке содержимого найденного (возможность вернуть владельцу потерянную вещь).

Претекстинг.

Так как данный метод раскручивается по определенному сценарию, то рассмотрим распространенные мошеннические схемы:

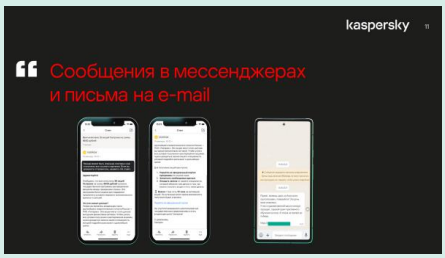


- Получение какого-либо SMS с информацией неблагоприятного характер. Для разрешения поставленной проблемы требуется, в большинстве случаев, сделать денежный перевод на указанный в сообщении телефонный номер и ни при каких обстоятельствах не выходить на контакт с данным человеком.
- Звонки от банков, управляющих компаний и т.д. Телефонные мошенники используют такой сценарий, чтобы ответы жертвы можно было использовать в своих целях (оформление кредитов, микро-займов и т.д.). Во многих случаях, параллельно телефонному разговору, требуется выполнение дополнительных действий, таких как ввод данных банковской карты на определенном сайте, установка какого-либо приложения и т.д.
- Использование нейросетей для подделки голоса, внешности пользователя. Чаще всего мошенники создают поддельный аккаунт в мессенджерах или социальных сетях и для правдоподобности присылают голосовые сообщения, в которых голос совпадает с начальником, руководителем подразделения и т.д., суть сообщения – выполнения определенных действий, которые маскируются под благое дело, а фактически – потеря денежных средств или личных аккаунтов в социальных сетях, мессенджерах.



Учащиеся рассматривают конкретные ситуации, анализируют их и формулируют тактику по защите от воздействия социальной инженерии мошенников.

Рекомендуется работа в группах с дальнейшей общей дискуссией.

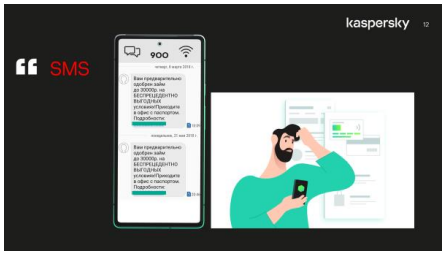


Ситуация: получение на электронную почту письма, которое информирует нас о зачислении денежных средств, предварительно требующее заполнения личных данных и банковских карт.

Ситуация: получение в мессенджере сообщения с просьбой проголосовать за родственника в конкурсе.

Данные ситуации относятся к фишингу. В первом случае жертва может потерять денежные средства и персональные данные, во втором – доступ к личному аккаунту, так как в таких формах

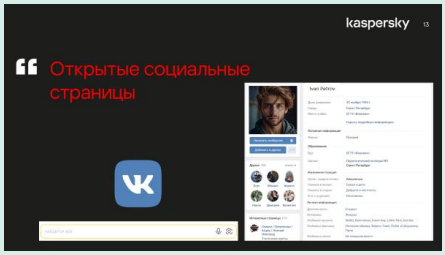
голосований требуют авторизацию через аккаунт мессенджера или социальной сети.



Ситуация: получение SMS об одобренном займе на выгодных условиях.

Получение сообщений с уведомлениями о займе, который не запрашивали, может вызвать беспокойство. Такие ситуации могут быть связаны с различными факторами, включая мошенничество, ошибки в системе кредитования или утечку личных данных.

Если лично не запрашивали такой информации, то следует игнорировать такие сообщения. При возникновении вопросов и сомнений, свою кредитную историю можно проверить через специализированное бюро, обратиться в которое можно через госуслуги.



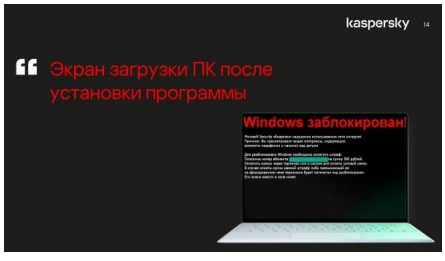
Ситуация: личные страницы социальных сетей с подробным заполнением данных о себе в публичном доступе.

Вся личная информация, которая опубликована в открытом доступе, может быть использована мошенниками в разной степени. Это может быть сбор всей личной информации на одного человека из разных источников для проработки какой-либо схемы, которые будут включать шантаж, создание дублирующего фейкового аккаунта, подготовку информации для обработки жертвы психологическими методами (втереться в доверие для упрощения проведения мошеннической операции).

В этом случае учащимся предлагается произвести поиск по картинке – главной личной фотографии, которая опубликована в социальных сетях. Можно воспользоваться поисковыми машинами от Яндекс или Google.

Найденная личная информация за счет поиска по картинке должна насторожить учащихся. А цель проделанной работы – задуматься о том, какую информацию они публикуют и как максимально безопасно произвести настройки публичности своих страниц.

Многие социальные сети предлагают гибкую настройку публичности, с предварительным просмотром. Рекомендуется закрыть полный доступ от незарегистрированных пользователей. А максимальную открытость информации можно предоставить только тем, кто «находится в друзьях».

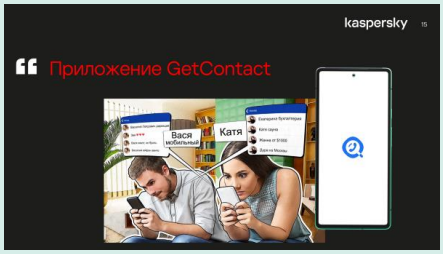


Ситуация: после установки приложения ПК перезагрузился и выдает сообщение на экране о недопустимом поведении в Интернете и требовании о переводе денежных средств на указанный номер.

Данная ситуация возникает, если произошла установка ПО из ненадежного источника. В этом случае делать какие-либо переводы бессмысленно, так как разблокировки ПК не будет.

Рекомендуется попробовать удалить вредоносное ПО из автозагрузки системы через безопасный режим, с последующим его устранением при помощи специализированных приложений, стерев всевозможные следы установки такого файла из системы.

Следует отметить, что не всегда вредоносное ПО такого плана не загружается в безопасном режиме.



Ситуация: установка приложения GetContact.

За последнее время практически все пользователи телефонов сталкивались со спам-звонками.

Разработчики мобильных приложений взяли это желание на заметку: кто-то предлагает указывать при звонке репутацию номера, кто-то – указывать информацию о компании, которой он принадлежит, а кто-то – сразу блокировать.

Среди таких решений особенно популярно в последнее время приложение GetContact, которое определяет незнакомые номера при помощи адресных книг самих пользователей.

Оно позволяет мгновенно заносить в черный список спамеров, легко блокировать нежелательные звонки, искать контакты по имени или номеру.

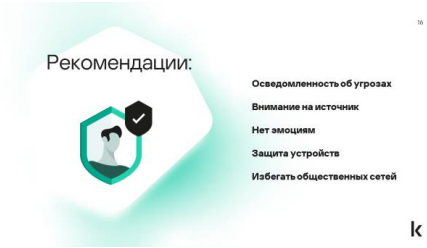
Для полноценного функционирования приложения требуется поделиться своей записной книжкой, со всеми номерами и именами контактов. Поэтому GetContact часто используют не по назначению. По всему миру пользователи активно проверяют свои номера, чтобы узнать, как их называют знакомые.

А как же приватность? На сайте производителя GetContact опубликовано положение о конфиденциальности, согласно которому пользователь предоставляет приложению доступ к любым личным и корпоративным данным, в том числе хранящимся в других программах и соцсетях, а оно имеет право делиться ими с третьими лицами. То есть, принимая эти условия, пользователи добровольно отправляют в сеть персональные данные, причем не только свои, но и всех своих знакомых.

Авторы приложения утверждают, что не продают свою базу. Но пользовательским соглашением предусмотрена возможность передачи данных третьим лицам, также в нем прописан пункт о согласии пользователя на получение рассылок.

Из-за спорной политики конфиденциальности GetContact уже официально запретили в некоторых странах, например в Казахстане и Азербайджане.

Прекращение использования приложения не влечет удаление ранее переданных данных, сервис уже собрал пару миллиардов телефонов пользователей из разных стран.



Рекомендации, которые позволят не поддаться воздействиям методов социальной инженерии:

- Осведомленность об угрозах.
  Чем чаще мы осведомлены о различных событиях и ситуациях, тем больше мы к ним готовы, видя схожий сценарий проводимых манипуляций со стороны мошенников.
- Внимание на источник.
  Не переходим по сомнительным ссылкам, которые приходят в сообщениях или на электронную почту.
- Нет эмоциям.
  Если оппонент требует от нас мгновенных действий, то лучше взять паузу и обдумать, какие последствия могут быть. Не позволять незнакомым контактам манипулировать нашими эмоциями.
- Защита устройств.
  Устанавливаем приложения по защите личного информационного пространства, которые в своем функционале могут проверять не только вредоносные приложения, но и спам, ссылки и сайты.
- Избегать общественных сетей.
  Подключаться к общественным сетям только в крайних случаях необходимости. А при онлайн покупке или авторизации на каких-либо сервисах использовать VPN, чтобы передаваемые данные были защищены методами шифрования.

Подводим итоги занятия.

Контрольные вопросы:

- С каким новым понятием мы познакомились на занятии?
- Какие основные методы, которые используют мошенники, можно выделить в социальной инженерии?
- Как можно защитить свое личное информационное пространство от мошенников?
- Будет ли полезна рассмотренная информация вашим родственникам и знакомым?

Благодарим за внимание.

www.kaspersky.com/
www.securelist.com