СӘТБАЕВ УНИВЕРСИТЕТІ

SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 6

Социальная инженерия

Преподаватель: **Батыргалиев Асхат Болатканович, PhD,**
ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»

askhat.b.b@gmail.com

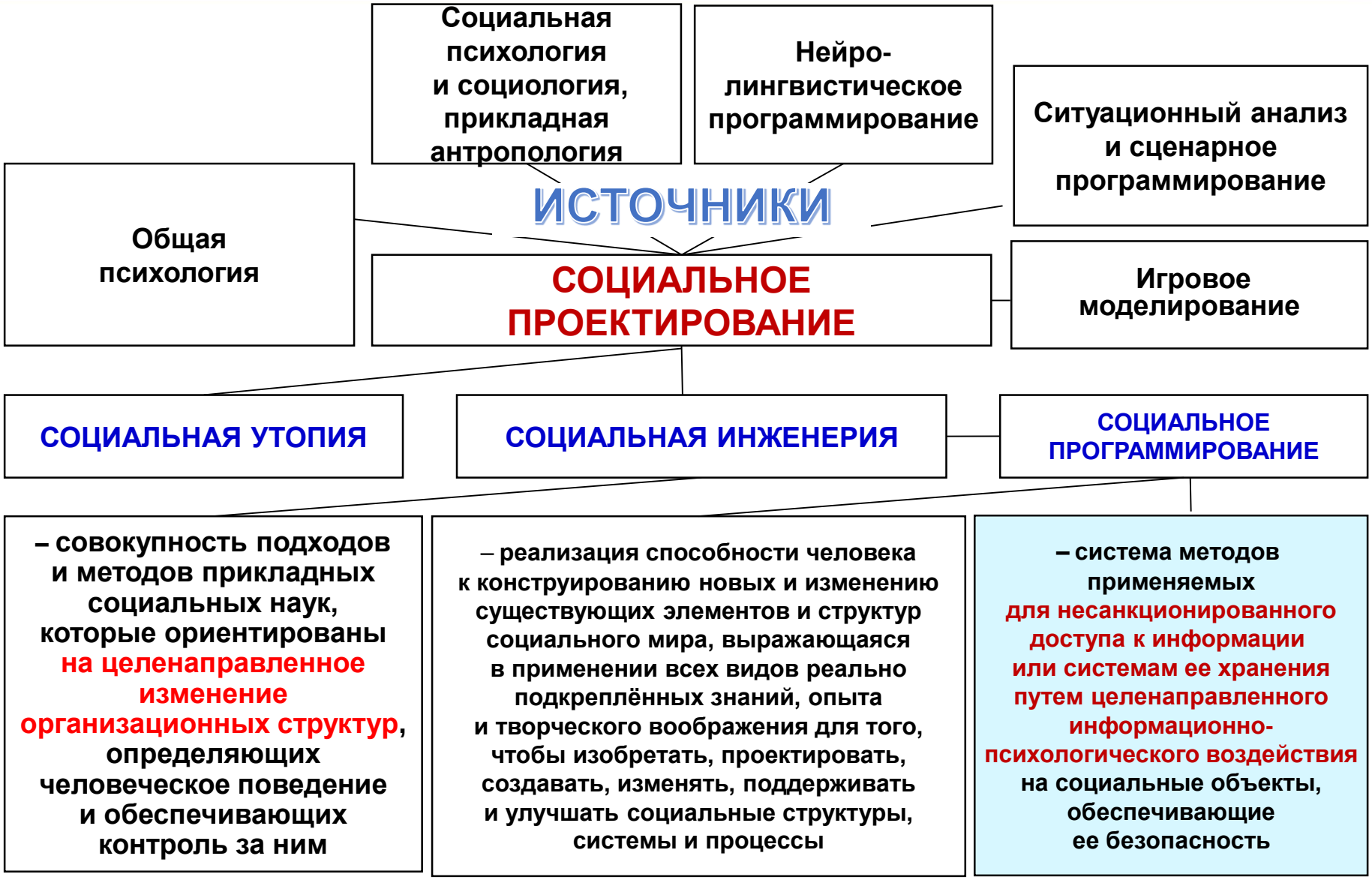
Содержание

1. Сущность социальной инженерии
2. Деструктивные методы и приемы социальной инженерии и защита от них

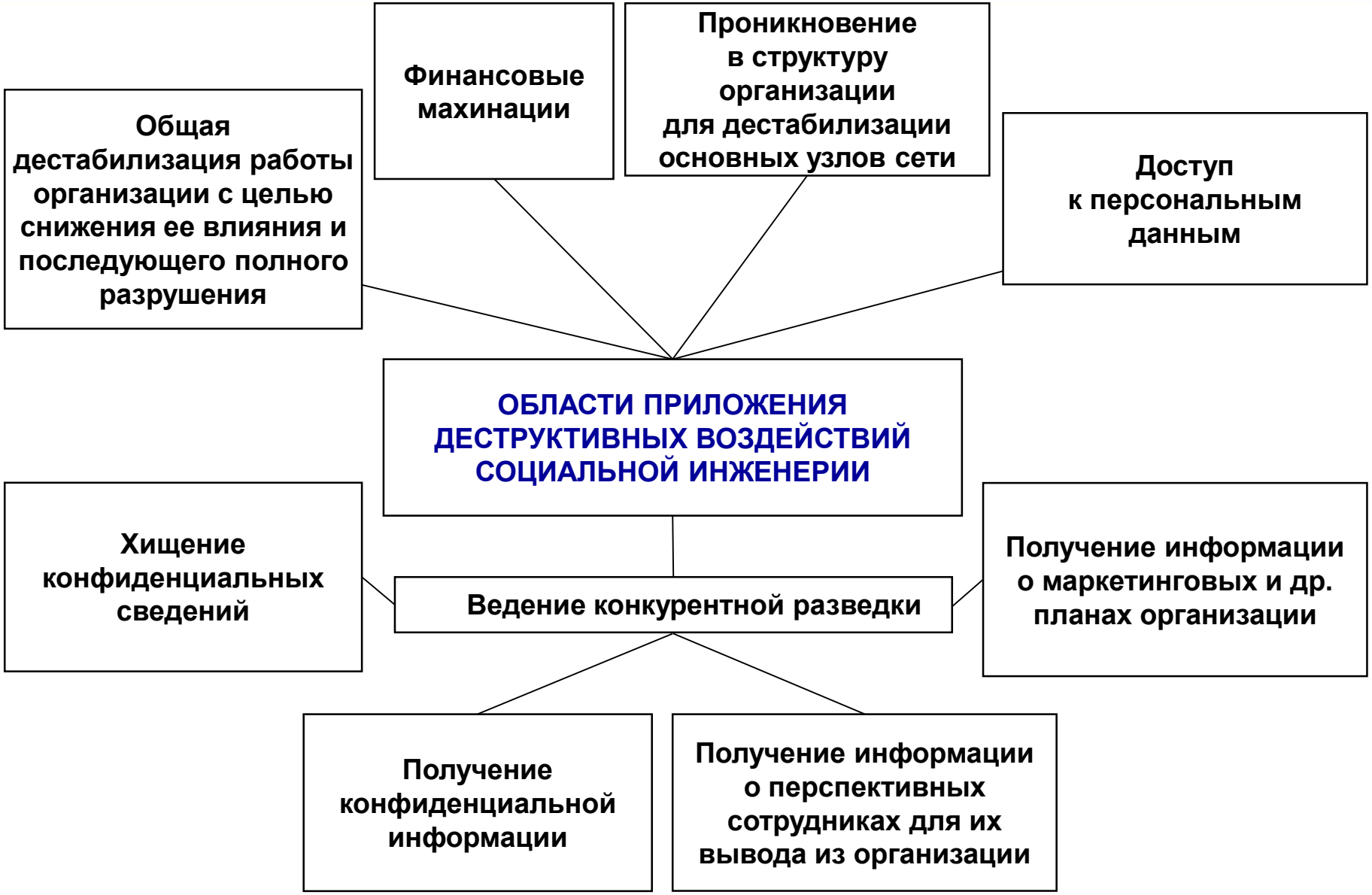
По завершению урока Вы будете знать:

1. Сущность социальной инженерии
2. Деструктивные методы и приемы социальной инженерии и защита от них

Подходы к определению сущности социальной инженерии



Задачи привлечения методов социальной инженерии для информационных воздействий



Деструктивные аспекты применения методов социальной инженерии

ОБМАН СОТРУДНИКА (системного администратора, секретаря в приемной, оператора call-центра, менеджера по работе с клиентами, охранника на посту, адресата почты или телефонного вызова)

QUID PRO QUO

IVR (телефонный фишинг)

ФИШИНГ

PRETEXTING

ПРОНИКНОВЕНИЕ НА ТЕРРИТОРИЮ

ВЫЯСНЕНИЕ И ПОЛУЧЕНИЕ ТЕЛЕФОННЫХ НОМЕРОВ, ПАРОЛЕЙ, СВЕДЕНИЙ

ПЛЕЧЕВОЙ СЕРФИНГ

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ОТКРЫТЫХ КАНАЛОВ ТЕЛЕКОММУНИКАЦИЙ
(телефон, электронная почта, фальшивые интернет-сайты, служба мгновенного обмена СМС, социальные сети)

ПРЯМАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

ИЗУЧЕНИЕ И АНАЛИЗ ИНФОРМАЦИОННОЙ СФЕРЫ ОБЪЕКТА

ОБРАТНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

НЕСАНКЦИОНИРОВАННАЯ СМЕНА ПАРОЛЕЙ

ОРГАНИЗАЦИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ И БАЗАМ ДАННЫХ

ПОДБРОС ИНФИЦИРОВАННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ («ДОРОЖНОЕ ЯБЛОКО»)

СОЗДАНИЕ УЧЕТНЫХ ЗАПИСЕЙ (С ПРАВАМИ ПОЛЬЗОВАТЕЛЯ ИЛИ АДМИНИСТРАТОРА)

ВНЕДРЕНИЕ ТРОЯНСКИХ ПРОГРАММ

ТЕХНОЛОГИЧЕСКОЕ ВСКРЫТИЕ И ПРИМЕНЕНИЕ СПОСОБОВ УДАЛЕННОГО ДОСТУПА

НЕСАНКЦИОНИРОВАННОЕ ДОБАВЛЕНИЕ ДОПОЛНИТЕЛЬНЫХ ПРАВ И ВОЗМОЖНОСТЕЙ ЗАРЕГИСТРИРОВАННЫМ ПОЛЬЗОВАТЕЛЯМ СИСТЕМЫ

Угрозы безопасности, связанные с электронной почтой и с использованием службы мгновенного обмена сообщениями

	ФАКТОРЫ	СПОСОБЫ ЗАЩИТЫ
ЭЛЕКТРОННЫЕ ПИСЬМА	Объем корреспонденции, когда невозможно уделить должное внимание каждому письму	Привитие скептического отношения к неожиданным входящим письмам
	Жертва часто выполняет запрос, не задумываясь о своих действиях	Включение в политику безопасности принципов использования электронной почты, применительно к: ❖ вложениям в документы; ❖ гиперссылкам в документах; ❖ запросам личной или корпоративной информации, исходящим изнутри предприятия; ❖ запросам личной или корпоративной информации, исходящим извне предприятия
	Гиперссылки, позволяющие доступ неавторизованных пользователей к корпоративным ресурсам или запрашивающие данные	
SMS	Неформальный характер общения в сочетании с возможностью присваивать себе любые имена позволяет злоумышленнику выдавать себя за другого человека	Выбрать одну платформу для мгновенного обмена сообщениями. Определить параметры защиты, задаваемые при развертывании службы SMS. Определить принципы установления новых контактов. Задать стандарты выбора паролей. Составить рекомендации по использованию службы SMS
	Вероятность указания ссылки на вредоносную программу в теле сообщения	
	Вероятность доставки вредоносной программы	

Вторжения и меры противодействия

Средства и силы вторжения	Телефон, электронная почта, сеть Интернет, СМС	Рекламные буклеты, справочники, визитки, сайты с информацией	Посетители

СПОСОБЫ И ПРИЕМЫ ВТОРЖЕНИЙ

Представление себя известным лицом, коллегой, знакомым или от их имени, или новым сотрудником

Использование детальной информации (названий структур, отделов, должностей, фамилий руководителей и сотрудников, их перемещений), из открытых источников (справочников), придающей речи правдивый характер

Невинная фраза, произнесенная злоумышленнику охранником: бухгалтер в отпуске. С помощью ТС осуществляется доступ к локальной сети, направляется сообщение от имени бухгалтера со своего компьютера, что работа – дома, и набирается номер приемной. Секретарь зная, что бухгалтер в отпуске, переводит звонок на системного администратора. Тот, услышав от секретаря, что на проводе бухгалтер, дает ему доступ к нужному документу.

Создание ситуации, когда предписанный сотрудником порядок реагирования оказывается неприменимым (об оказании срочной помощи, отсутствии лица, отпуске)

Обращение (например, в кадровую службу) под именем сотрудника государственной организации, (военкома-та) с просьбой предоставить персональные данные

Попытки через администратора установить удаленный доступ к документам хитростью, когда социальный инженер выдает себя за кадрового работника, шантажом и даже с использованием романтических чувств

Обращения посетителей к охранникам под любым невинным предлогом и вызывающим сочувствие (бабушки, женщины с детьми, инвалиды – «к медсестре, в туалет, помыть руки»)

Вторжения и меры противодействия

МЕРЫ ПРОТИВОДЕЙСТВИЯ

Воспрещение произнесения лишней информации ни при каких обстоятельствах и никому – в пункте инструкции

Проверка обращающегося лица требованием назвать кодовое слово, ежедневно сменяемое руководством

Организация тестовых попыток проникновения с участием людей, которых персонал не знает

Исключение избыточной информации на сайте, в рекламных буклетах, СМИ, визитках

Запрет на разглашение телефонов сотрудников и других данных о них

Проведение разъяснительных бесед о том, что персональные данные ни в коем случае нельзя разглашать по телефону, даже если на том конце якобы находится сотрудник уполномоченной организации

Собеседования с сотрудниками об опасности вторжений и реальности ущерба

Воспитание и сплачивание коллектива

Своевременные обновления справочников с уточнением данных об убывших и новых сотрудниках

Обучение сотрудников (особенно операторов, кассиров, охранников, секретарей) задавать уточняющие вопросы, проверять ответы любым способом (перезванивая, обеспечивая контроль над электронной почтой и пр.), не переводить внешние звонки на внутреннюю линию, записывать данные всех посторонних обращающихся

Организация проверок пропускного режима и работы охранников с посетителями

Фишинг (Целевой фишинг)

Массовая или индивидуальная отправка сообщений по электронной почте пользователю с целью убедить его выполнить какое-либо действие (в т.ч. проверку данных) и записать последовательность, а также установить вредоносное ПО для последующего проникновения и получения корпоративной интеллектуальной собственности или конфиденциальной информации (логинов, паролей и пр.)

Подготовка сообщения злоумышленником					
Подбор конкретной, информации о человеке или компании	Персонализация - модификация электронного сообщения под конкретного пользователя, якобы полученного из надежного (или располагающего доверием) источника	Обеспечение высокого качества орфографии и грамматики сообщения	**Направление сообщения**	**Получение и чтение послания**	**Следование пользователем рекомендациям, обозначенным в тексте сообщения**

Фишинг (Целевой фишинг)

ПРИЗНАКИ ФИШИНГ- АТАК

Получение сведений – по телефону (IRV), электронной почте, онлайн объявлениях, в социальных сетях, в результатах поисковых систем, всплывающих системных сообщениях операторов, СОДЕРЖАЩИХ:

- предупреждения, вызывающие беспокойство
- угрозы
- обещания
- запросы о пожертвованиях
- грамматические или пунктуационные ошибки
- поздравления с успехом, победой, выигрышем
- напоминание о необходимости изменения учетных данных
- уведомления о потенциальных заражениях и предложения установки антивирусных программ («scareware»)

ПРИМЕНЕНИЕ ТЕЛЕФОННОГО ФИШИНГА (вишинг – англ. vishing – voice fishing)

- Подбор конкретной, информации о человеке или компании
- Предварительная запись голосовых сообщений, с целью воссоздать «официальные звонки» банковских и др. IVR систем
- Получение жертвой запроса связаться с банком и подтвердить или обновить какую-либо информацию
- Получение требования системы о аутентификации пользователя вводом PIN-кода или пароля, выполнения типичной команды: «Нажмите единицу, чтобы сменить пароль. Нажмите двойку, чтобы получить ответ оператора» создав впечатление работающей в данный момент системы предварительно записанных сообщений

Претекстинг (Pretexting)

Использование голосовых средств связи (телефон, Skype и т.п.) для получения информации от имени третьего лица или с уверением, что кто-то нуждается в помощи – чаще всего по отношению к нетехническим пользователям, которые могут владеть полезной информацией

Использование небольших запросов и упоминание имен реальных людей в организациях, обычно вышестоящих	Объяснение, что некто нуждается в помощи, на основании того, что большинство готово исполнить небольшие просьбы, которые не воспринимаются как подозрительные запросы	После установления доверительной связи – просьба более существенного, обычно и с большим успехом.

ПРИЗНАКИ:

проявление собеседником к вам повышенного интереса, преувеличенного внимания и заботы	отказ сообщить вам свои координаты	обращение к вам со странной или необычной просьбой	попытка втереться к вам в доверие или лесть	подчеркнуто начальственный тон

ПРЕДСТАВЛЕНИЯ СОТРУДНИКОВ КАК КРИТИЧЕСКИ ВАЖНЫЕ УЯЗВИМОСТИ:

сотрудники считают, что корпоративная система безопасности непогрешима	сотрудники теряют бдительность	сотрудники легко верят полученной информации, независимо от ее источника	сотрудники не дооценивают значимость информации, которой владеют	сотрудники искренне хотят помочь каждому, кто об этом просит	сотрудники не осознают пагубных последствий своих действий	сотрудники считают соблюдение корпоративной политики безопасности пустой тратой времени и сил

Иные виды социальной инженерии

ПЛЕЧЕВОЙ СЕРФИНГ

(англ. shoulder surfing) – наблюдение личной информации жертвы через её плечо в общественных местах (кафе, торговые центры, аэропорты, вокзалы, в общественном транспорте)

QUID PRO QUO («то, за что» - «услуга за услугу»)

обращение злоумышленника в компанию по корпоративному телефону или электронной почте

ПРИЗНАКИ:

злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении	в процессе «решения» технических проблем, злоумышленник вынуждает цель совершать действия, позволяющие запускать команды или устанавливать различное программное обеспечение на компьютере «жертвы»	большинство офисных работников готовы разгласить конфиденциальную информацию (свои пароли), за услугу или вознаграждение

Ограничения использования снифферов

СБОР ИНФОРМАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

из социальных сетей (Twitter, Facebook, Qzone, Google+, Instagram, Sina Weibo, LinkedIn, Last.fm, MySpace, Livejournal, Now, ЯRUS, TenChat, Яндекс. Дзен, Одноклассники, ВКонтакте, Мой Мир и др.)

«ДОРОЖНОЕ ЯБЛОКО»

Осуществляется подбрасывание «инфицированных» носителей информации (CD, флеш-накопитель), на которых записана программа, инициирующая атаку клиентской рабочей станции или сети при ее открытии, - в места общего доступа (туалеты, парковки, столовые, рабочее место атакуемого сотрудника, на полу лифта или в вестибюле). Вредоносное ПО находится внутри Excel, Word или PDF файлов, а сами устройства помечаются, привлекающими внимание надписями («Финансовый отчет», «Прайс-лист», «Строго конфиденциально» и т.д.), снабжаются корпоративным логотипом и ссылкой на официальный сайт компании.

Сотрудник по незнанию может подобрать диск и поместить его в компьютер, чтобы удовлетворить своё любопытство.

Троянские программы

Троянская программа – вредоносная программа удаленного доступа, сбора, разрушения, модификации информации, дезактивации программ безопасности, использования ресурсов, направляемая жертве в форме электронного сообщения (ссылки), содержащего привлекательный контент (обновление антивируса и др.)

ЦЕЛИ

закачивание и скачивание файлов	копирование ложных ссылок, ведущих на поддельные вебсайты, чаты или другие сайты с регистрацией	создание помех работе пользователя	похищение данных, представляющих ценность или тайну, в том числе информации для аутентификации, несанкционированного доступа к ресурсам, которые могут быть использованы в преступных целях	сбор адресов электронной почты и использование их для рассылки спама

уничтожение данных (стирание или переписывание данных на диске, трудно замечаемые повреждения файлов), выведения из строя или отказа обслуживания компьютерных систем, сетей	наблюдение за пользователем и тайное сообщение третьим лицам сведений (например, привычка посещения сайтов)	регистрация нажатий клавиш с целью кражи информации о паролях и номерах кредитных карточек	дезактивация или создание помех работе антивирусных программ и файервола

Троянские программы

ПРИЗНАКИ

нарушение работы других программ (вплоть до повисания компьютера, решаемого лишь перезагрузкой, и невозможности их запуска)	имитация имени и интерфейса существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных, как для запуска пользователем, так и для маскировки в системе своего присутствия	настойчивое, независимое от владельца предложение в качестве стартовой страницы спам-ссылок, рекламы или порносайтов	распространение по компьютеру пользователя порнографии	превращение языка текстовых документов в бинарный код	предложение сделать определённое действие для предотвращения трудно поправимого следствия (бессрочной блокировки пользователя со стороны сайта, потери банковского счета, получения доступа к управлению компьютером, установки вредоносного ПО)

Обратная социальная инженерия

Жертва сама предлагает нужную информацию злоумышленнику (лицу, обладающему авторитетом в технической или социальной сфере, которое часто получает важную личную информацию, в том числе, когда никто не сомневается в их порядочности: сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль – им не нужна эта информация – однако, многие пользователи ради скорейшего устранения проблем добровольно сообщают эти сведения).

ПРИЗНАКИ

Злоумышленник, работающий вместе с жертвой, изменяет на её компьютере имя файла или перемещает его в другой каталог

•Жертва замечает пропажу файла.
•Злоумышленник заявляет, что может все исправить, но только войдя в систему с учетными данными жертвы.
• Жертва, желая быстрее завершить работу или избежать наказания за утрату информации, соглашается.

Жертва просит злоумышленника войти в систему под её именем, чтобы попытаться восстановить файл

Злоумышленник:
•неохотно соглашается и восстанавливает файл;
•крадет идентификатор и пароль жертвы;
•успешно осуществив атаку, улучшает свою репутацию, и вполне возможно, что после этого к нему будут обращаться за помощью и другие коллеги.

Этот подход не пересекается с обычными процедурами оказания услуг поддержки и осложняет поимку злоумышленника

Несанкционированное проникновение

Получение злоумышленником физического доступа
на объект путем принуждения
или обмана сотрудников,
или в обход периметра безопасности

Получение злоумышленником конфиденциальных данных
и (или) установка крытых устройств съема информации в очень
короткий промежуток времени

Фотографирование документов, оставленных на принтерах или столах,
или установка устройств, обеспечивающих последующий
Wi-Fi или 3G доступ к сети

Анализ и предотвращение обмана методами социальной инженерии

Прежде доступ к информации был признаком высокого положения и привилегии. В настоящее время всё, чем занимаются служащие, связано с обработкой информации. Поэтому не только руководители, располагающие информацией, а работники всех уровней могут быть мишенью, особенно новички в группе обслуживания клиентов

ПОДХОДЫ К АНАЛИЗУ

Люди полностью уязвимы перед обманом, поскольку могут изменить отношение в сторону доверия к собеседнику, если манипулировать ими определенным образом

Социальный инженер ожидает подозрение и недоверие, и он всегда подготавливается, чтобы недоверие превратить в доверие.

Социальный инженер создает проблему, а потом чудесным образом ее решает, обманом заставляя жертву предоставить доступ к самым охраняемым секретам

Мы судим людей по телефону точно так же, как и обычно – бессознательно, в спешке, во время первых секунд разговора: собеседник дружелюбный и общительный или чувствуется враждебность или давление, говорит ли он как образованный человек?

Человеку свойственно предполагать, что вряд ли его обманут именно в этой конкретной ситуации, по крайней мере, пока нет причин предполагать обратное.

Мы взвешиваем риски и затем, в большинстве случаев, доверяем без всяких сомнений.

Анализ и предотвращение обмана методами социальной инженерии

ПОДХОДЫ К НЕЙТРАЛИЗАЦИИ ОБМАНА МЕТОДАМИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Уяснить твердо, что звонящий или посетитель не является тем, за кого он себя выдает только потому, что он знает имена некоторых людей в компании, корпоративные терминологию или процессы.

Полагать это подозрительным.

Отказаться от привычки формировать свое мнение о человеке или компании по качеству Интернет-сайта, внешности, одежде, манере разговора и др. внешним данным.

В современных условиях это может ничего не значить с точки зрения безопасности

Избавиться от привычки доводить персональную или служебную информацию кому-либо, кроме своего руководства по его требованию, а подчиненных, – по мере крайней необходимости.

Задачи ставятся в отсутствие посторонних относительно содержания задач лиц.