Социотехническое тестирование

С чего начинается социотехническое тестирование?

- время на подготовку к тестированию
- условия, которые должна обеспечить компания для старта работ

- объем разведывательных работ
- формат тестирования

- стоимость тестирования

Для чего и как проводить такое тестирование?

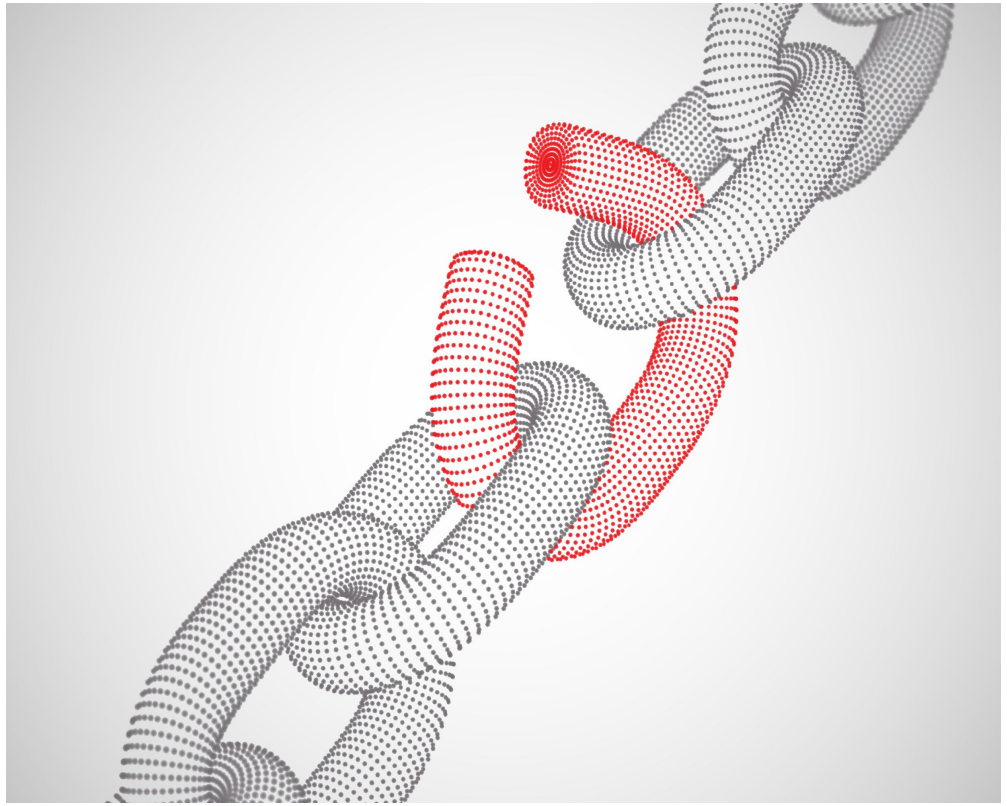
Социотехническое тестирование может проводиться для установления:

•уровня осведомленности сотрудников и их практических навыков в распознавании социотехнических атак

•эффективности функционирования систем обеспечения информационной безопасности

•уровня подготовки сотрудников ИТ- и ИБ-отделов к выявлению и реагированию на социотехнические атаки (уровень осведомленности в вопросах безопасности данных сотрудников выше, что повышает сложность тестирования)

•возможности компрометации инфраструктуры (социотехническое тестирование может применяться для тестирования на проникновение)



Соотношение цели социотехнического тестирования (социальная инженерия или СИ) и других его составляющих

	Определить уровень подготовленности сотрудников	**Определить эффективность функционирования СЗИ**	**Определить уровень подготовленности сотрудников ИТ- и ИБ-отделов**	**Компрометация инфраструктуры**
Формат тестирования	· письма со ссылкой на поддельный ресурс (фишинг) · письма с исполняемым вложением (нагрузка) · телефонное взаимодействие (вишинг)	· письма со ссылкой на поддельный ресурс (фишинг) · письма с исполняемым вложением (нагрузка)	· письма со ссылкой на поддельный ресурс (фишинг) · письма с исполняемым вложением (нагрузка) · телефонное взаимодействие (вишинг)	· письма со ссылкой на поддельный ресурс (фишинг) · письма с исполняемым вложением (нагрузка)
Начальные условия	· ФИО сотрудников и email-адреса · номера телефонов, ФИО и/или должности сотрудников, а также любая другая информация согласно легенде · добавление в белые списки (email-адреса, домены, СЗИ и т.д.)	· ФИО сотрудников и email-адреса	· ФИО сотрудников и email-адреса · номера телефонов, ФИО и/или должности сотрудников, а также любая другая информация согласно легенде · добавление в белые списки (email-адреса, домены, СЗИ и т.д.)	· входная информация не предоставляется
Время на подготовку	Одна неделя	Две недели	Одна-две недели	Три недели

Различные ошибки и просто любопытные моменты

Ошибки, влияющие на результаты тестирования.

> *Представим, что в компании N проводится несколько социотехнических тестирований, каждое из которых включает телефонное взаимодействие с сотрудниками. Список сотрудников и их контакты предоставлял представитель компании.*
>
> *Первое телефонное взаимодействие было успешным: ряд сотрудников, поддавшись на уговоры эксперта, совершили потенциально опасные действия.*
>
> *Второе тестирование тоже: сотрудники поверили легенде и охотно выполнили все, о чем их попросили.*
>
> *А вот третье тестирование закончилось, не успев начаться. Уже на втором звонке легенда была раскрыта, сотрудник сказал, что дважды на одну удочку не попадется и оповестит о тестировании всех сотрудников, включая службу безопасности. Тестирование пришлось остановить.*
>
> *Шок! Как так? Поиск ошибки начали с повторной проверки списка сотрудников, заявленных на каждое из трех тестирований. Совпадений нет. Потом проверили номера телефонов… И вот он — один номер телефона, только в первом тестировании он заявлен для Ивановой Анны Сергеевны, а в третьем — для Петровой Анны Сергеевны (здесь и далее используются вымышленные имена). За время, прошедшее между тестированиями, девушка сменила фамилию.*
>
> *В ходе первого тестирования Иванова Анна Сергеевна поверила в легенду и выполнила все действия, следуя указаниям эксперта, а вот Петрова Анна Сергеевна быстро поставила на место нерадивого эксперта.*
>
> *Получается, что ошибка была допущена на этапе подготовки: эксперт проверил только фамилии сотрудников, но проигнорировал номера телефонов.*

Форматы социотехнического тестирования

В проектах использовались следующие форматы социотехнического тестирования:

1) рассылка фишинговых писем со ссылкой на поддельный ресурс — 52%
2) рассылка фишинговых писем с исполняемым вложением — 36%
3) телефонные звонки (вишинг) — 12%

Высокая результативность вишинга объясняется следующими моментами:

- Заранее известна информация, которую нужно получить
- Большой объем работ по сбору информации о сотрудниках и компании, которая используется для формирования легенды и сценария разговора
- В разговоре используется информация, которая указывает на осведомленность эксперта во внутренних процессах компании
- Эксперт демонстрирует эмоциональную заинтересованность в сложившейся ситуации или схожие интересы, чтобы притупить внимание собеседника

Кейс №1

Цель: получить информацию разной степени критичности (компания определила информацию, которую считала конфиденциальной).
Легенда: сотрудника уведомляют об инциденте ИБ — его пропуск использовали для несанкционированного прохода через СКУД в хранилище М. Служба безопасности расследует инцидент и звонит, чтобы узнать текущее местоположение пропуска, где находился пропуск в рабочее время, существуют ли альтернативные способы для прохождения СКУД. Звонят в нерабочее время (выходной день). Эксперт должен убедить сотрудника проверить доменную учетную запись на факт компрометации — сотрудника просят аутентифицироваться на резервном портале (фишинговый ресурс).

Количество участников и инфраструктура под спойлером

Количество участников: 50 человек.
Инфраструктура: поддельный домен, поддельный корпоративный портал, который при вводе учетных данных перенаправлял сотрудника на оригинальный портал.

Вернемся к Татьяне Игоревне и информации, которую она предоставила за время разговора:

использует пропуск и специальный браслет для прохождения СКУД

пропуск и браслет находятся дома

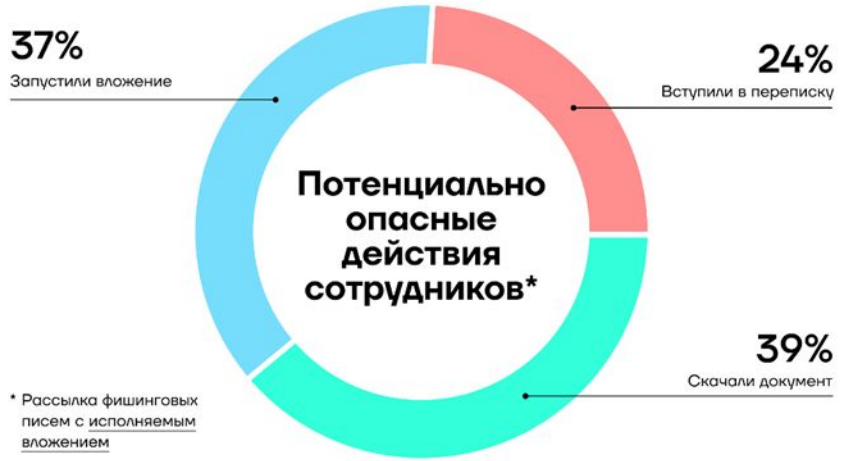
использует корпоративную электронную почту дома

предоставила свои учетные данные, введя их на фишинговом ресурсе:
02.03.2020 13:48:25#0.2.0.2#ida****:rsa****55#Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 YaBrowser/19.3.1.828 Yowser/2.5 Safari/537.36

Компания остановила тестирование сотрудников после того как:

- 29 телефонных взаимодействий было нами произведено;
- 23 сотрудника раскрыли конфиденциальную информацию различного уровня критичности.

Какие могут быть результаты



Кейс №2

Цель: оценить осведомленность сотрудников в вопросах информационной безопасности.

Легенда: ознакомиться с новой системой премирования. К письму прилагался документ «Премии.xls».

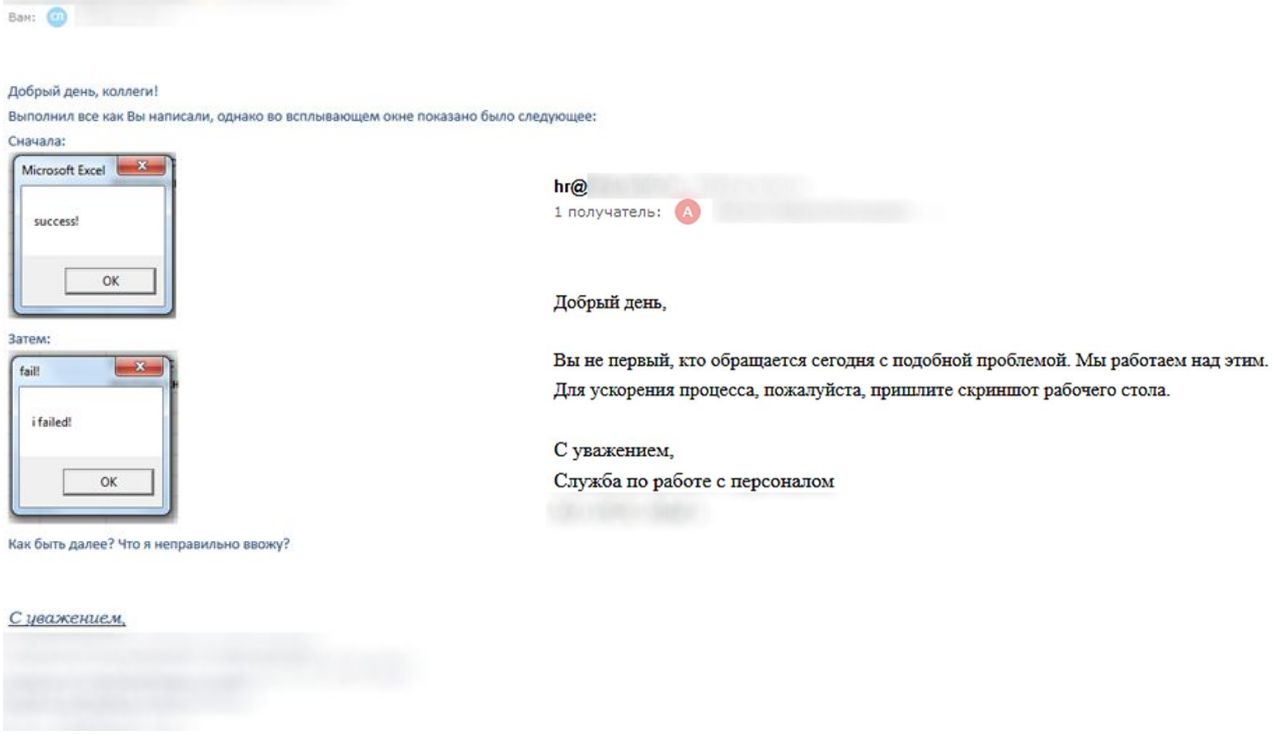
Количество участников и инфраструктура под спойлером

Количество участников: 75 человек.

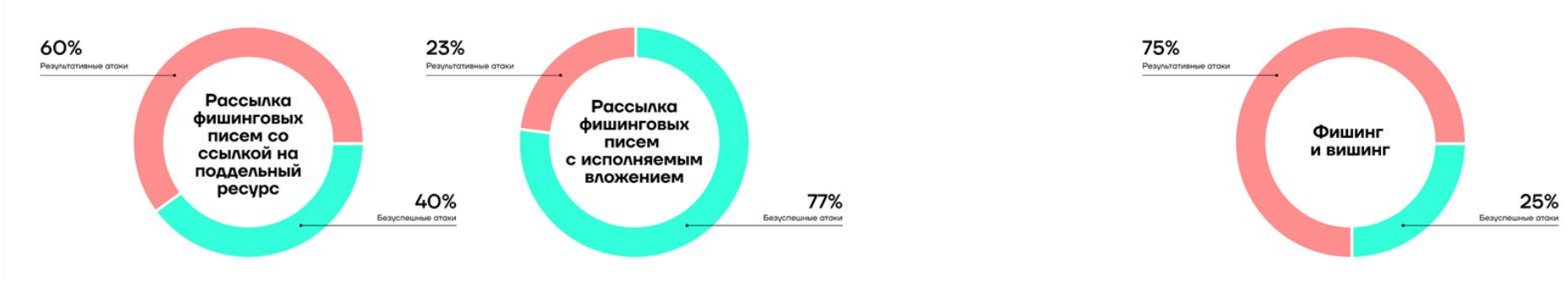
Инфраструктура: поддельный домен, поддельный почтовый адрес (якобы принадлежащий отделу по работе с персоналом), вредоносная нагрузка, которая выполнялась в ОС удаленного компьютера, обеспечивала соединение с ним и собирала данные о конфигурации ОС.

За время тестирования удалось успешно подключиться к компьютерам 11 сотрудников (14% участников). Столкнувшись якобы с проблемой в работе документа, сотрудники вступали в переписку с экспертами — в том числе и не заявленные в тестировании сотрудники.

ПРИМЕР ПЕРЕПИСКИ



Возвращаемся к тенденциям



Легенды

Ниже представлены основные примеры легенд:

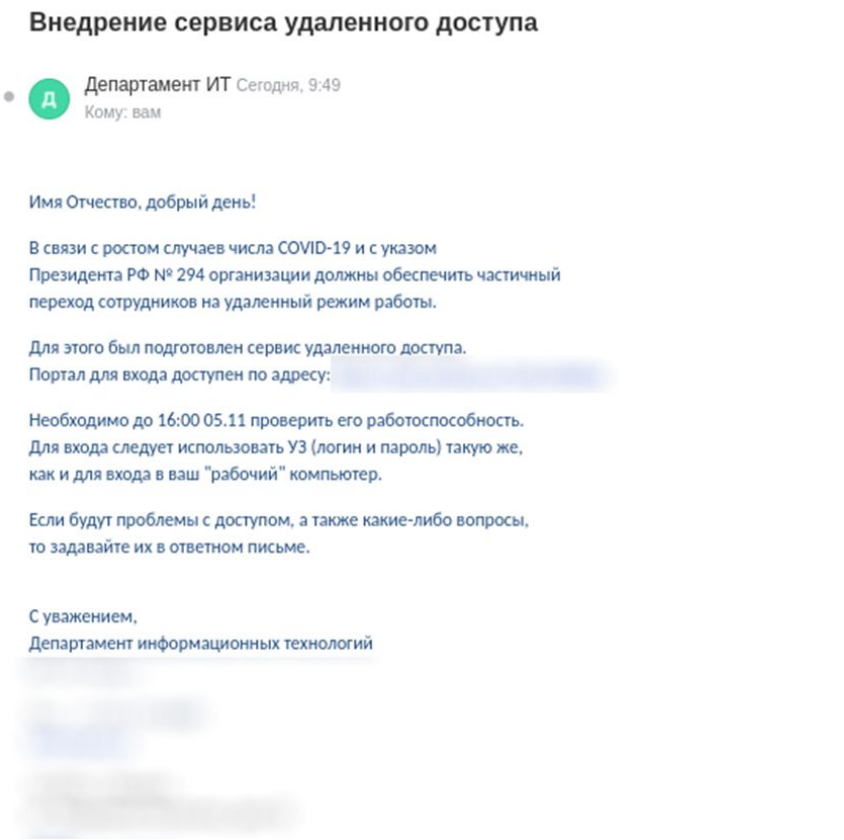
- Изменение в графике работы
- Изменение в IT-системах
- Система премирования
- Скидки и бонусы
- События в компании

Кейс №3

Цель: оценить осведомленность сотрудников в вопросах информационной безопасности.
Легенда: проверить сервис удаленного доступа, поскольку сотрудники переходят на удаленную работу из-за COVID-19. Для проверки доступа надо ввести учетные данные от рабочего компьютера на фишинговой странице, которая копировала страницу входа на VPN-портал.

Количество участников и инфраструктура под спойлером

Количество участников: 150 человек.
Инфраструктура: поддельный домен, поддельный почтовый адрес (якобы принадлежащий ИТ-отделу), поддельная страница входа на VPN-портал.



Внедрение сервиса удаленного доступа

Департамент ИТ Сегодня, 9:49
Кому: вам

Имя Отчество, добрый день!

В связи с ростом случаев числа COVID-19 и с указом Президента РФ № 294 организации должны обеспечить частичный переход сотрудников на удаленный режим работы.

Для этого был подготовлен сервис удаленного доступа.
Портал для входа доступен по адресу:

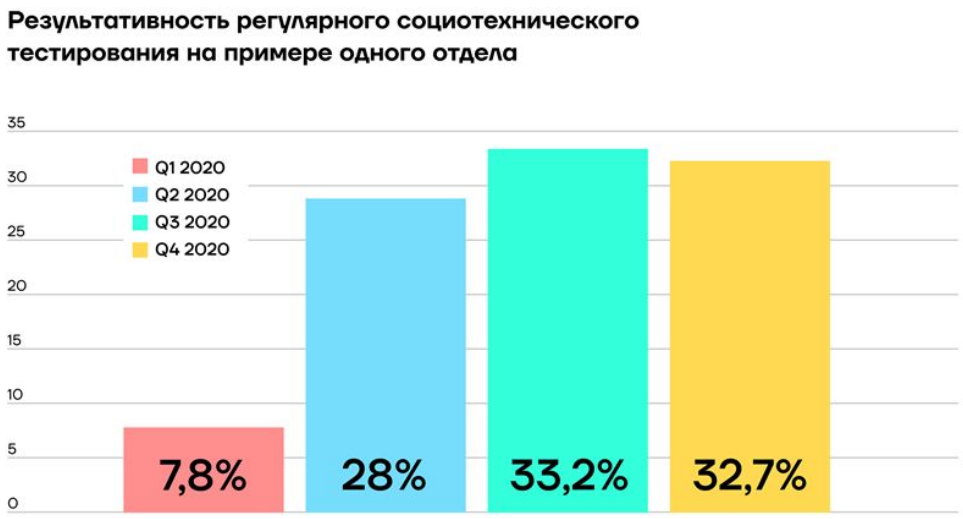
Необходимо до 16:00 05.11 проверить его работоспособность.
Для входа следует использовать УЗ (логин и пароль) такую же, как и для входа в ваш "рабочий" компьютер.

Если будут проблемы с доступом, а также какие-либо вопросы, то задавайте их в ответном письме.

С уважением,
Департамент информационных технологий

Ход и результаты рассылки на тему COVID-19

Кейс №4



Компания М время от времени организовывала социотехническое тестирование своих сотрудников. Какого-то ощутимого прогресса в знаниях основ информационной безопасности не наблюдалось: сотрудники продолжали переходить по ссылкам, вступать в переписку и выполнять просьбы.

Чтобы продемонстрировать, что положительная динамика возможна только при регулярном тестировании, решили провести четыре социотехнических тестирования в течение года (в начале каждого квартала). Все тестирования проводились в одном формате, но под разными легендами, а участвовали в них сотрудники одного подразделения.

Результат регулярного тестирования оказался таким же, как и у нерегулярного: сотрудники переходили по ссылкам, вступали в переписку и раскрывали конфиденциальную информацию. Результативность отдельного тестирования в большей степени определялась актуальностью легенды. В 3 квартале легенда с COVID-19 заставила людей забыть о тренингах, наставлениях и рекомендациях.

Кейс №5

В этом примере демонстрируем, как выявленное на ранних этапах социотехническое тестирование оказалось результативным только из-за того, что сотрудники, распознавшие тестирование, не оповестили о нем коллег.

Цель: получить валидные учетные данные сотрудников.
Легенда: проверить наличие доступа к новому корпоративному порталу.

Количество участников и инфраструктура под спойлером

Количество участников: 200 человек.
Инфраструктура: поддельный домен, поддельный почтовый адрес (якобы принадлежащий отделу техподдержки), поддельный корпоративный портал, который при вводе учетных данных перенаправлял сотрудника на оригинальный портал.

Активная фаза социотехнического тестирования началась 11 февраля 2020 года в 13:30 (МСК).

Первые учетные данные мы получили через 4 минуты:

Дата и время	IP-адрес / MAC-адрес	Введенные логин и пароль	Общая информация о конфигурации рабочей станции
11.02.2020 13:34	0.0.0.1	ni*********a:V******v	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
11.02.2020 13:34	0.0.0.6	mi****a:2******aB3	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Примерно через 30 минут после начала тестирования получили данные, явно указывающие, что легенда раскрыта и сотрудники либо догадались о проводимом тестировании, либо заподозрили атаку: вместо учетных данных в логах собиралась ненормативная лексика.

Дата и время	IP-адрес / MAC-адрес	Введенные логин и пароль	Общая информация о конфигурации рабочей станции
11.02.2020 14:02	0.0.0.71	Idi ** *** sobaka:ahahhahaha	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.75 Safari/537.36

Кейс №5

Тестирование можно сворачивать и садиться за отчет, но сотрудники продолжали вводить учетные данные. Последний ввод данных был зафиксирован 17 февраля. Следовательно, сотрудники, распознавшие тестирование (или атаку), не предупредили об этом своих коллег.

Дата и время	IP-адрес / MAC-адрес	Введенные логин и пароль	Общая информация о конфигурации рабочей станции
17.02.2020 14:08	0.0.0.55	Ty********v:T**********rah	Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1

Всего получили 76 уникальных учетных данных. Валидность каждой пары была подтверждена.

Итоги, проблемы и рекомендации

Следует помнить о:

- регулярном обучении и опросе сотрудников
- понятной поставке материалов и гайдов (Вики-страницы, видео и т.п.)
- обязательной двухфакторной аутентификации
- разграничении доступа и минимизации прав пользователей
- хорошей фильтрации электронной почты
- средствах защиты от целенаправленных атак

СПАСИБО ЗА ВНИМАНИЕ!