Лекция 4: Социальная инженерия и человеческий фактор

Тема: Вредоносное ПО и социальная инженерия

Технический университет Молдовы

Лектор: Максим Масютин

Введение

Добро пожаловать. На предыдущей лекции мы рассмотрели технический мир вредоносного ПО. Сегодня мы сосредоточимся на том, что специалисты по безопасности часто называют самым слабым звеном любой системы защиты: человеческом факторе.

Социальная инженерия — это искусство манипулирования людьми с целью заставить их совершить определённые действия или раскрыть конфиденциальную информацию.

Если технические атаки эксплуатируют уязвимости программного обеспечения, то социальная инженерия эксплуатирует психологию человека. И, как оказывается, человеческая психология имеет множество уязвимостей, которые невозможно устранить программными обновлениями.

Статистика весьма показательна. Согласно отчёту Verizon Data Breach Investigations Report за 2025 год, человеческий фактор присутствует примерно в 60 процентах всех нарушений безопасности.

Центр жалоб на интернет-преступления (IC3) при ФБР зафиксировал 859 532 обращения в 2024 году с общим ущербом в 16,6 миллиарда долларов, что на 33 процента больше по сравнению с предыдущим годом.

Пожалуй, наиболее тревожно следующее: фишинговые письма, сгенерированные ИИ, имеют показатель кликабельности в 54 процента, что значительно превышает 12-процентный показатель кликабельности фишинговых писем, составленных человеком. Сочетание искусственного интеллекта и социальной инженерии создаёт угрозы беспрецедентной сложности.

Рассмотрим, как работают эти атаки и как мы можем защититься от них.

Часть 1: Психология социальной инженерии

Социальная инженерия успешна, потому что эксплуатирует фундаментальные аспекты человеческой психологии. Понимание этих принципов помогает распознавать манипуляции и противостоять им.

Принципы влияния

Психолог Роберт Чалдини выделил шесть принципов влияния, которые социальные инженеры регулярно эксплуатируют:

1. Взаимность

Люди чувствуют себя обязанными отвечать на оказанные услуги. Если кто-то делает что-то для нас, мы чувствуем потребность сделать что-то в ответ.

Пример атаки: Злоумышленник, выдающий себя за сотрудника IT-поддержки, "помогает" сотруднику с вымышленной проблемой, а затем просит его пароль как часть "решения". Сотрудник чувствует себя обязанным выполнить просьбу после получения "помощи".

2. Последовательность и приверженность

Как только мы берём на себя обязательство, мы склонны выполнять его, чтобы выглядеть последовательными.

Пример атаки: Злоумышленник сначала получает небольшое согласие ("Вы можете подтвердить, что работаете в бухгалтерии?"), а затем повышает ставки ("Раз вы в бухгалтерии, вы можете одобрить этот срочный банковский перевод, верно?").

3. Социальное доказательство

Мы ориентируемся на действия других людей для определения правильного поведения, особенно в ситуациях неопределённости.

Пример атаки: "Все остальные в вашем отделе уже обновили свои пароли по этой ссылке. Вы последний."

4. Авторитет

Мы склонны выполнять просьбы авторитетных лиц или тех, кто производит впечатление авторитетности.

Пример атаки: Электронное письмо, якобы от генерального директора, требует немедленных действий. Сотрудники не решаются подвергать сомнению авторитет, особенно в условиях дефицита времени.

5. Симпатия

Мы с большей вероятностью выполняем просьбы людей, которые нам нравятся или кажутся привлекательными.

Пример атаки: Злоумышленники устанавливают доверительные отношения через дружескую беседу перед тем, как обратиться с просьбой. Они могут исследовать цели, чтобы найти общие интересы.

6. Дефицит

Мы ценим вещи больше, когда они редки или доступны в течение ограниченного времени.

Пример атаки: "Это обновление безопасности доступно только в течение следующих 30 минут, после чего ваша учётная запись будет заблокирована." Давление времени препятствует тщательному обдумыванию.

Дополнительные психологические факторы

Страх и срочность

Страх запускает реакцию "бей или беги", которая снижает аналитическое мышление. Срочные запросы эксплуатируют это, требуя немедленных действий.

"Ваша учётная запись была скомпрометирована! Нажмите здесь немедленно, чтобы защитить её, или потеряете все свои данные!"

Любопытство

Люди от природы любопытны. Мы хотим увидеть, что находится за завесой.

"Вы не поверите, что ваш коллега сказал о вас в этом видео..."

Жадность

Обещание получить что-то бесплатно апеллирует к нашему стремлению к выгоде.

"Вы выиграли бесплатный iPhone! Просто введите свои данные, чтобы получить его."

Готовность помочь

Большинство людей хотят быть полезными. Злоумышленники эксплуатируют это, прося об "одной маленькой услуге".

"Я не могу войти в свою учётную запись и мне очень нужно отправить этот отчёт начальнику. Можете просто быстро войти за меня?"

Часть 2: Фишинговые атаки

Фишинг — это наиболее распространённая форма социальной инженерии, использующая обманные сообщения для того, чтобы заставить получателей раскрыть информацию или совершить вредоносные действия.

Фишинг по электронной почте

Традиционный фишинг использует массовую рассылку электронных писем от имени легитимных организаций:

- Банки, запрашивающие верификацию учётной записи
- Поставщики услуг, предупреждающие о блокировке учётной записи
- Службы доставки с уведомлениями об отправке
- IT-отделы, требующие сброса паролей

APWG зафиксировала более одного миллиона фишинговых атак в первом квартале 2025 года — это наибольший квартальный показатель с конца 2023 года.

Характеристики фишинговых писем:

- Ощущение срочности
- Общие приветствия ("Уважаемый клиент")
- Подозрительные адреса отправителей
- Грамматические и орфографические ошибки (хотя ИИ устраняет этот индикатор)
- Несовпадающие или подозрительные URL-адреса
- Запросы конфиденциальной информации

Целевой фишинг

Целевой фишинг направлен на конкретных людей с использованием персонализированной информации. В отличие от массового фишинга, целевой фишинг тщательно исследует своих жертв.

Злоумышленники собирают информацию из:

- Профилей в социальных сетях
- Веб-сайтов компаний
- Контактов в LinkedIn
- Открытых источников
- Ранее произошедших утечек данных

Целевое фишинговое письмо может ссылаться на:

- Вашу настоящую должность и отдел
- Недавние объявления компании
- Имена ваших коллег или руководителей
- Проекты, над которыми вы работаете
- Конференции, которые вы посещали

Такая персонализация значительно увеличивает вероятность успеха.

Уэйлинг

Уэйлинг нацелен на высокопоставленных лиц, как правило, на руководителей или лиц, обладающих финансовыми полномочиями. Эти атаки тщательно исследуются и продуманно готовятся.

Типичные сценарии уэйлинга:

- Поддельные срочные запросы от генерального директора
- Мошеннические юридические уведомления
- Поддельные документы о слияниях и поглощениях
- Материалы заседаний совета директоров

Руководители становятся мишенью, потому что:

- Имеют полномочия одобрять транзакции
- Имеют доступ к конфиденциальной информации
- Могут обладать меньшей осведомлённостью в области технической безопасности
- Часто слишком заняты для тщательной проверки

Компрометация деловой переписки (BEC)

Атаки **BEC** используют имитацию деловых партнёров для манипулирования сотрудниками с целью перевода средств или раскрытия информации.

Типичные сценарии BEC:

- **Мошенничество от имени руководителя**: Поддельный запрос руководителя на банковский перевод
- **Имитация поставщика**: Поддельный счёт с изменёнными реквизитами оплаты
- **Имитация юриста**: Срочное юридическое дело, требующее оплаты
- **Компрометация учётной записи**: Злоумышленник использует реально скомпрометированную учётную запись электронной почты

BEC причинил убытки на миллиарды долларов. Одна успешная атака может привести к переводу миллионов до момента обнаружения.

Часть 3: Голосовые атаки (вишинг)

Вишинг (голосовой фишинг) использует телефонные звонки для манипулирования жертвами. С развитием клонирования голоса на основе ИИ вишинг стал значительно более опасным.

Традиционный вишинг

Классические атаки вишинга включают:

- Поддельные звонки от технической поддержки ("Мы обнаружили вирус на вашем компьютере")
- Имитацию налоговых органов
- Имитацию отдела банковской безопасности
- Мошенничество с призами и лотереями

Вишинг эффективен, потому что:

- Разговор в реальном времени создаёт давление
- Идентификатор вызывающего абонента может быть подделан
- Голос передаёт авторитет и срочность
- Проверка сложнее, чем в случае с электронной почтой

Вишинг с использованием ИИ

Ландшафт угроз кардинально изменился с появлением клонирования голоса на основе ИИ. Атаки вишинга возросли на 442 процента в конце 2024 года благодаря дипфейкам на основе ИИ.

Как работает вишинг с использованием ИИ:

1. Злоумышленники собирают образцы голоса из открытых источников (видеозаписей, подкастов, конференц-звонков)
2. Модели ИИ клонируют голос с высокой точностью
3. Злоумышленники звонят сотрудникам, выдавая себя за руководителей
4. Генерация голоса в реальном времени делает разговоры убедительными

Реальный случай: В феврале 2024 года финансовый работник инженерной фирмы Arup перевёл 25 миллионов долларов мошенникам после участия в, казалось бы, легитимной видеоконференции. Каждое лицо на экране было реальным, каждый голос идеально совпадал, но все они были дипфейками, сгенерированными ИИ, — злоумышленники клонировали голоса и лица руководителей, используя общедоступные видеоматериалы.

Вишинг теперь затрагивает 30 процентов организаций, а имитация руководителей с использованием дипфейков выросла на 15 процентов.

Часть 4: Текстовые атаки (смишинг)

Смишинг (SMS-фишинг) использует текстовые сообщения для проведения атак. По мере того как люди становятся более подозрительными к электронной почте, злоумышленники переключаются на SMS.

Почему смишинг работает

- Более высокий процент открытия, чем у электронной почты (более 90%)
- Маленькие экраны затрудняют проверку URL-адресов
- Менее развитая фильтрация спама на мобильных устройствах
- Люди доверяют текстовым сообщениям больше, чем электронной почте
- Ощущение немедленности

Типичные атаки смишинга

- Банковские оповещения о подозрительных транзакциях
- Уведомления о доставке со ссылками для отслеживания
- Уведомления о призах или вознаграждениях
- Запросы на верификацию учётной записи
- Кража кодов двухфакторной аутентификации

Техники смишинга

Мошенничество с доставкой посылок: "Ваша посылка не может быть доставлена. Перенесите доставку здесь: [вредоносная ссылка]"

Банковские оповещения: "Обнаружена подозрительная активность на вашем счёте. Подтвердите немедленно: [ссылка]"

Обход MFA: "Ваш код подтверждения: 123456. Если вы не запрашивали его, позвоните по номеру [номер злоумышленника]"

Часть 5: Фишинг через QR-коды (квишинг)

Квишинг использует QR-коды для проведения фишинговых атак. Фишинг через QR-коды вырос более чем на 500 процентов по мере распространения корпоративной "нормализации QR-кодов".

Почему квишинг работает

- QR-коды скрывают целевой URL-адрес
- Пользователи не могут предварительно просмотреть ссылку перед сканированием
- Смартфоны могут не отображать полные URL-адреса
- Корпоративное внедрение QR-кодов нормализовало их сканирование
- Обходит фильтры безопасности электронной почты

Сценарии квишинга

Физический квишинг:

- Поддельные штрафы за парковку с QR-кодами для "оплаты"
- Вредоносные QR-коды, размещённые поверх легитимных
- QR-коды в поддельных официальных уведомлениях

Цифровой квишинг:

- QR-коды в фишинговых письмах (обходят текстовые фильтры)
- Поддельные уведомления об истечении срока двухфакторной аутентификации
- QR-коды в корпоративных документах

Реальные примеры:

- Поддельные штрафы за парковку в Сан-Франциско, перенаправляющие на сайты кражи учётных данных

- Мошенничество с QR-кодами в Вашингтонском университете с кражей учётных данных
- Поддельные письма об истечении срока двухфакторной аутентификации Microsoft с QR-кодами

Защита от квишинга

- Используйте сканеры QR-кодов с предварительным просмотром URL
- С подозрением относитесь к неожиданным QR-кодам
- Проверяйте физические QR-коды на предмет подмены
- По возможности вводите URL-адреса вручную

Часть 6: Многоканальные атаки

Современные злоумышленники больше не полагаются на одноканальные атаки. Вместо этого они создают сложные схемы с использованием множества точек контакта для укрепления доверия.

Как работают многоканальные атаки

1. **Первоначальный контакт**: Электронное письмо подтверждает "срочное обновление безопасности"
2. **Подкрепление**: SMS-напоминание о той же проблеме
3. **Социальное подтверждение**: Сообщение в LinkedIn от поддельного IT-коллеги
4. **Эскалация**: Сообщение в Teams/Slack, выражающее обеспокоенность
5. **Финальное давление**: Звонок с дипфейковым голосом "руководителя", требующего действий

После множества точек контакта жертвы с гораздо большей вероятностью поверят запросу, поскольку он был "подтверждён" через различные каналы.

Характеристики

- Последовательное повествование через все каналы
- Каждая точка контакта подкрепляет легитимность
- Давление времени нарастает на протяжении всей атаки
- Множество кажущихся независимыми источников подтверждают срочность
- Эксплуатирует нашу склонность доверять подтверждённой информации

Часть 7: ИИ в социальной инженерии

Искусственный интеллект превратил социальную инженерию из трудоёмкого ремесла в индустриализированную угрозу.

Фишинг, сгенерированный ИИ

Отчёт о тенденциях фишинговых угроз за 2025 год указывает, что 82,6 процента фишинговых писем, проанализированных в период с сентября 2024 по февраль 2025 года, содержали контент, сгенерированный ИИ.

К октябрю 2025 года фишинг, сгенерированный ИИ, стал главной угрозой для корпоративной электронной почты, превзойдя программы-вымогатели, внутренние угрозы и традиционную социальную инженерию вместе взятые.

Почему фишинг на основе ИИ эффективен:

- Безупречная грамматика и орфография
- Контекстуально уместное содержание
- Персонализация в масштабе
- Имитация стиля письма персоны, за которую выдаёт себя злоумышленник
- Генерация уникальных вариаций для обхода фильтров

Цифры: Фишинговые письма, сгенерированные ИИ, имеют показатель кликабельности 54 процента по сравнению с 12 процентами для писем, составленных человеком.

Технология дипфейков

Аудиодипфейки клонируют голос на основе образцов:

- Конференц-звонки, интервью и подкасты служат исходным материалом
- Генерация в реальном времени позволяет вести живые разговоры
- Качество продолжает быстро улучшаться

Видеодипфейки создают убедительное поддельное видео:

- Имитация участников виртуальных совещаний
- Поддельные видеообращения от руководителей
- В сочетании с клонированием голоса обеспечивают полную имитацию личности

Теневая торговля инструментами для создания дипфейков в даркнете выросла на 223 процента между первым кварталом 2023 и первым кварталом 2024 года.

Генеративный ИИ в рабочих процессах злоумышленников

На протяжении 2025 года генеративный ИИ стал центральным элементом операций злоумышленников:

- Более убедительный фишинг, сгенерированный ИИ
- Ускоренная автоматизированная разведка
- Мошеннические схемы, усиленные синтетическими медиа
- Снижение порога входа для злоумышленников

Более 86 процентов организаций уже столкнулись как минимум с одним фишинговым инцидентом или инцидентом социальной инженерии, связанным с ИИ.

Часть 8: Физическая социальная инженерия

Социальная инженерия выходит за пределы цифровых каналов и распространяется на физические атаки.

Претекстинг

Претекстинг создаёт сфабрикованный сценарий для вовлечения жертв. Злоумышленник принимает ложную личность с правдоподобной предысторией.

Примеры:

- Выдача себя за сотрудника IT-поддержки для получения доступа в здание
- Имитация курьера
- Притворство новым сотрудником
- Выдача себя за аудитора или инспектора

Эффективные претексты включают:

- Подробную предысторию
- Соответствующий внешний вид и реквизит
- Уверенность и авторитет
- Знание организационных деталей

Проход следом и проход вслед за другим

Проход следом (tailgating) — это следование за авторизованным лицом через защищённый вход.

Техники:

- Несение коробок (отговорка "заняты руки")
- Ношение одежды, похожей на униформу сотрудников
- Появление в часы пик при входе
- Имитация поиска пропуска

Проход вслед за другим (piggybacking) аналогичен, но происходит с ведома авторизованного лица (которое придерживает дверь из вежливости).

Приманка

Приманка (baiting) — это оставление заражённых носителей для того, чтобы жертвы нашли и использовали их.

Типичные приманки:

- USB-накопители с надписью "Конфиденциально" или "Информация о зарплатах"
- CD- или DVD-диски, оставленные в общих зонах
- Устройства с логотипами компании

Любопытство побуждает жертв подключать найденные устройства, что приводит к установке вредоносного ПО.

Анализ мусора

Поиск ценной информации в мусоре:

- Выброшенные документы
- Старое оборудование с данными
- Стикеры с паролями
- Организационные схемы и справочники

Надлежащие политики уничтожения документов противодействуют этой угрозе.

Часть 9: Стратегии защиты

Защита от социальной инженерии требует сочетания технических мер, политик и повышения осведомлённости персонала.

Обучение по информационной безопасности

Наиболее эффективная защита — это обученные пользователи, которые распознают атаки и противостоят им.

Обучение должно охватывать:

- Распознавание признаков фишинга
- Процедуры верификации необычных запросов
- Сообщение о подозрительных действиях
- Безопасное обращение с неожиданными контактами
- Реальные примеры и сценарии

Подходы к обучению:

- Регулярные информационные занятия
- Симуляция фишинговых кампаний
- Геймификация и вовлечение
- Немедленная обратная связь при ошибках
- Метрики отслеживания прогресса

Процедуры верификации

Установите процедуры для проверки необычных запросов:

Внеполосная верификация:

- Обратный звонок по известным номерам (не по номерам, указанным в подозрительных сообщениях)
- Использование альтернативных каналов связи
- Верификация через установленные контакты

Многостороннее одобрение:

- Крупные транзакции требуют множественных подтверждений
- Конфиденциальные действия требуют подтверждения руководителя
- Банковские переводы имеют обязательные процедуры подтверждения

Технические меры

Хотя социальная инженерия нацелена на людей, технические меры помогают:

Безопасность электронной почты:

- Фильтры спама и фишинга
- Аутентификация DMARC, DKIM, SPF

- Предупреждения о внешних письмах
- Защита ссылок и использование песочницы

Безопасность телефонии:

- Процедуры верификации вызывающего абонента
- Обучение распознаванию подделки идентификатора вызывающего абонента
- Запись конфиденциальных звонков

Управление доступом:

- Многофакторная аутентификация
- Системы управления посетителями
- Обязательное использование пропусков для входа

Создание культуры безопасности

Долгосрочная защита требует культурных изменений:

- Сделать безопасность ответственностью каждого
- Устранить стигматизацию при сообщении об ошибках
- Поощрять поведение, ориентированное на безопасность
- Руководство демонстрирует приверженность
- Регулярное информирование об угрозах

Часть 10: Практические упражнения

Разберём несколько сценариев для применения изученного материала.

Сценарий 1: Анализ подозрительного письма

Вы получаете электронное письмо:

```
From: IT-Security@yourcompany.com.suspicious-domain.com
Subject: URGENT: Password Expiration in 24 Hours

Dear Employee,

Your corporate password will expire in 24 hours. To prevent account
lockout, please update your credentials immediately using the secure
link below:

[Update Password Now]
```

```
Failure to act will result in loss of access to all company systems.

IT Security Team
```

Тревожные признаки:

- Несоответствие домена (suspicious-domain.com);
- Общее приветствие ("Dear Employee");
- Давление срочности;
- Угроза последствий;
- Подозрительная ссылка.

Правильная реакция: Не нажимайте на ссылку. Сообщите в отдел IT-безопасности. Если вас беспокоит истечение срока пароля, уточните через официальные каналы IT.

Сценарий 2: Верификация телефонного звонка

Вам звонят. Звонящий утверждает, что он из отдела безопасности вашего банка: "Мы обнаружили подозрительную активность на вашем счёте. Для подтверждения вашей личности, пожалуйста, назовите номер вашего счёта и последние четыре цифры вашего идентификационного номера."

Тревожные признаки:

- Незапрошенный звонок;
- Запрос конфиденциальной информации;
- Создание срочности по поводу "подозрительной активности".

Правильная реакция: Повесьте трубку. Позвоните в ваш банк по номеру, указанному на карте или в выписке. Никогда не предоставляйте конфиденциальную информацию в ответ на входящие звонки.

Сценарий 3: Запрос на банковский перевод от руководителя

Вы получаете электронное письмо от генерального директора с просьбой срочно перевести средства новому поставщику: "Мне нужно, чтобы вы немедленно выполнили банковский перевод на 50 000 долларов этому новому поставщику. Я на совещании и меня нельзя беспокоить. Это конфиденциально — не обсуждайте ни с кем."

Тревожные признаки:

- Срочность;
- Требование секретности;

- Необычный запрос от руководителя;
- Невозможность проверки через обычные каналы.

Правильная реакция: Следуйте установленным процедурам верификации независимо от предполагаемого отправителя. Свяжитесь с генеральным директором через известные каналы. Никогда не обходите процедуры верификации ради "срочных" запросов.

Заключение

Сегодня мы рассмотрели социальную инженерию и человеческий фактор:

1. **Психология манипуляции**: Принципы Чалдини и эмоциональные триггеры
2. **Разновидности фишинга**: Фишинг по электронной почте, целевой фишинг, уэйлинг, BEC
3. **Вишинг**: Голосовые атаки, усиленные клонированием голоса на основе ИИ
4. **Смишинг**: SMS-атаки с высоким процентом открытия
5. **Квишинг**: Фишинг через QR-коды, эксплуатирующий нормализацию использования QR
6. **Многоканальные атаки**: Скоординированные атаки через множество точек контакта
7. **Трансформация с помощью ИИ**: Генеративный ИИ делает атаки более убедительными и масштабируемыми
8. **Физические атаки**: Претекстинг, проход следом, приманка
9. **Стратегии защиты**: Обучение, процедуры верификации, технические меры, культура

Человеческий фактор всегда будет частью безопасности. Наша цель — не устранить участие человека, а наделить людей способностью распознавать манипуляции и противостоять им.

На следующей лекции мы рассмотрим модели управления доступом и управление идентификацией.

Вопросы для обсуждения

1. Как организации могут сбалансировать процедуры верификации безопасности с операционной эффективностью?
2. Какие этические вопросы возникают при проведении симуляций фишинговых кампаний?

3. Поскольку ИИ делает дипфейки всё более убедительными, какие новые методы верификации потребуются?

Благодарю за внимание. До встречи на следующем занятии.

Контрольные вопросы

1. Объясните шесть принципов влияния Чалдини и то, как каждый из них может быть использован в атаках социальной инженерии.
2. Сравните фишинг, целевой фишинг и уэйлинг. Что делает каждый из них эффективным?
3. Что такое компрометация деловой переписки (BEC) и почему она стала одним из наиболее финансово разрушительных типов атак?
4. Как ИИ и технологии дипфейков меняют ландшафт угроз социальной инженерии?
5. Опишите фишинг через QR-коды (квишинг). Почему он особенно эффективен в современных условиях?
6. Что делает многоканальные атаки социальной инженерии более опасными, чем одноканальные?
7. Какие элементы должна включать эффективная программа обучения по информационной безопасности?
8. Опишите три техники физической социальной инженерии и контрмеры для каждой из них.

Ключевые термины

- **Состязательный ИИ**: Атаки, направленные на системы безопасности на основе машинного обучения с целью обхода обнаружения или ложной классификации
- **Приманка (baiting)**: Оставление заражённых носителей или предложение привлекательных предметов для заманивания жертв
- **BEC**: Компрометация деловой переписки (Business Email Compromise) — атака с имитацией руководителей или партнёров для авторизации мошеннических транзакций
- **Мошенничество от имени руководителя**: Разновидность компрометации деловой переписки, при которой злоумышленники выдают себя за высшее руководство для авторизации мошеннических транзакций

- **Дипфейк**: Синтетические медиа, сгенерированные ИИ, убедительно имитирующие реальных людей
- **Анализ мусора**: Поиск полезной информации в выброшенных материалах
- **Фишинг**: Мошеннические сообщения, предназначенные для того, чтобы обманом заставить получателей раскрыть информацию или совершить вредоносные действия
- **Симуляция фишинга**: Контролируемые учения, проверяющие восприимчивость сотрудников к фишинговым атакам в рамках обучения по безопасности
- **Претекстинг**: Создание сфабрикованного сценария для манипулирования целью с целью получения информации или доступа
- **Квишинг**: Фишинговые атаки с использованием QR-кодов для перенаправления жертв на вредоносные сайты
- **Обучение по информационной безопасности**: Образовательные программы, предназначенные для обучения сотрудников распознаванию угроз безопасности и реагированию на них
- **Смишинг**: Фишинговые атаки на основе SMS-сообщений
- **Социальная инженерия**: Психологическое манипулирование людьми с целью заставить их совершить действия или раскрыть конфиденциальную информацию
- **Целевой фишинг**: Адресный фишинг, направленный на конкретных людей или организации
- **Проход следом (tailgating)**: Следование за авторизованным лицом через защищённый вход без надлежащих учётных данных
- **Вишинг**: Голосовые фишинговые атаки, как правило, с использованием телефонных звонков
- **Уэйлинг**: Фишинговые атаки, специально нацеленные на высшее руководство