Методы социальной инженерии и фишинга

Методы социальной инженерии направлены на использование человеческого фактора (человеческих слабостей и недостатков) с целью получения от пользователя защищаемой информации или его учетных данных.

Наиболее эффективным методом противодействия социальной инженерии является повышение осведомленности пользователей о методах социальной инженерии.

При личном и телефонном общении Пользователь должен убедиться, что разговаривает именно с тем человеком, за которого себя выдает собеседник. При личном или телефонном взаимодействии социальный инженер обычно использует следующие тактики:

- представившись сотрудником технической поддержки какого-либо сервиса или службы, социальный инженер сообщает Пользователю о какой-либо поломке или нарушении в функционировании того или иного необходимого в работе сервиса, вызывая тем самым панику и заставляя Пользователя сообщить свои учетные данные;
- представившись руководителем высокого ранга, социальный инженер изображает гнев и недовольство действием или бездействием Пользователя, вынуждая сообщить учетные данные или иную конфиденциальную информацию;
- представившись сотрудником организации, деятельность которой так или иначе может быть интересна Пользователю вынуждает сообщить учетную или иную конфиденциальную информацию;
- иные подобные тактики.

При взаимодействии через электронную почту, социальный инженер преследует одну из двух основных целей:

- заражение АРМ Пользователя вредоносным программным обеспечением через запуск приложенного к письму файла или переходом по вредоносной ссылке;
- переход Пользователя по поддельной ссылке, по которой находится точная копия формы авторизации легального сервиса и ввод в эту форму идентификационной информации (как правило, при первом вводе логина и пароля поддельная форма сообщает о неправильном вводе пароля и перенаправляет на настоящую форму авторизации сервиса).

Наиболее распространенные примеры применения методов социальной инженерии с использованием каналов электронной почты:

- письмо от налоговой инспекции с предложением установить из вложенного файла новые формы для сдачи налоговых деклараций;
- письмо из банка о просроченном платеже по кредиту, подробности во вложенном файле;
- письмо из суда о возбуждении административного/уголовного дела, подробности во вложении;

- письмо от провайдера об одностороннем изменении тарифного плана, подробности во вложении;
- письмо от банка (или любого другого учреждения) о блокировке учетной записи на сайте или личного кабинета, необходимо пройти по ссылке, ввести учетные данные и вручную разблокировать личный кабинет или учетную запись;
- письмо от сервиса электронной почты (gmail.com, mail.ru, yandex.ru и т. п.) о грядущей блокировке почтового ящика, об исчерпании свободного места и т. д., необходимо пройти по ссылке, ввести учетные данные и выполнить некоторые действия.

При работе с электронной почтой в контексте противодействия методам социальной инженерии Пользователь руководствуется следующей информацией:

- совпадение адреса отправителя электронного письма с доверенным адресом не является гарантией подлинности самого письма, поскольку поле «от кого» может быть подделано злоумышленником;
- любые письма с вложениями являются подозрительными;
- любые письма, в которых отсутствует альтернативная контактная информация отправителя (ФИО, должность, мобильный, рабочий телефон, почтовый адрес) являются подозрительными;
- при получении неожидаемого электронного письма с вложением или ссылкой от якобы доверенного отправителя, необходимо по альтернативным каналам связи (лично, по телефону, через мессенджер) уточнить факт отправки такого письма;
- государственные и иные организации (банки, операторы связи и т. д.) не уведомляют своих клиентов о каких-либо проблемах, исках, блокировках по электронной почте, это делается официальным письмом на бумажном носителе, через СМС (например, в случае подключенного онлайн банкинга) или по телефону;
- необходимо тщательно проверять корректность ссылок, по которым просят пройти в письме, чаще всего злоумышленники используют похожие, но другие доменные имена, чтобы ввести Пользователя в заблуждение, например, заменяя букву “b” на букву “d” или цифру “1” на букву “l” и наоборот.

Атаки социальных инженеров могут быть веерными (нацеленными на как можно большее число жертв), так и целенаправленными (нацеленными на конкретную организацию или на конкретного человека). В случае целенаправленных атак, социальный инженер изучает информацию о потенциальной жертве и об организации из открытых источников (сайт компании, сайты партнеров и контрагентов, электронные биржи труда, социальные сети, новостные ленты и прочие ресурсы). В случае, если о Пользователе публикуется информация в открытых источниках или он сам публикует информацию о своем месте работы, роде деятельности, должностных обязанностях, Пользователь должен быть готов к применению этой информации социальным инженером против него.