НЕКОТОРЫЕ ТЕХНИКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

М.В. Стержанов, А.И. Гридасов, В.Я. Анисимов, В.Н. Теслюк

Социальная инженерия представляет из себя совокупность методов получения необходимого доступа к информации, основанных на особенностях психологии людей.

Приемы социальной инженерии классифицируются как нетехнические, однако они могут эффективно сочетаться с широко известными приемами использования вредоносных вложений, скрытого внедрения программ и т. д.

Претекстинг – это набор действий, отработанных по определенному, заранее составленному сценарию (содержащему психологические ловушки), в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Зачастую данный вид атаки применяется по телефону, при этом злоумышленник действует максимально быстро, не оставляя времени на размышления. В начале общения злоумышленник пытается получить доверие при помощи использования заранее заготовленных данных (имя человека; номер автомобиля; адрес).

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей (например, пин-кодов, авторизационных данных). Мошенники создают поддельные сайты, мимикрирующие под хорошознакомые ресурсы. Основным видом фишинговых атак является рассылка поддельных писем, с просьбой срочно выполнить какие-либо действия, связанных с аккаунтом пользователя (разблокировка, обновление информации, получение выигрыша и т.д.). Пользователь направляется на страницу ввода ввода учетных данных.

Для предотвращения атак, основанных на техниках социальной инженерии, рекомендуется регулярно проводить инструктаж сотрудников о способах реализации данных угроз, а также учитывать данные угрозы при составлении политики информационной безопасности. Рекомендуется использовать почтовые антивирусы, которые производят постоянное автоматическое сканирование писем на предмет вредоносного программного обеспечения.