УДК 681.5.015

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ФИШИНГОВЫХ АТАК

Папков В.А., Чеботаревский Д.С.
Научный руководитель – Пелевин В.Ф., к.т.н., доцент
Могилёвский государственный университет продовольствия
г. Могилев, Республика Беларусь

Фишинг представляет собой противоправное действие, совершаемое с целью заставить то или иное лицо поделиться своей конфиденциальной информацией. Это метод из социальной инженерии, который направлен на воровство персональных данных, включая данные для входа в банковский аккаунт и номера кредитных карт. Это происходит, когда злоумышленник маскируется под проверенное лицо, например, работником банка. Организация, ставшая жертвой такой атаки, обычно несет серьезные финансовые потери в дополнение к снижению репутации и доверия потребителей. В зависимости от масштаба, попытка фишинга может перерасти в инцидент безопасности, от которого бизнесу будет сложно избавиться.

Исследованы следующие методы фишинга. Фишинговые рассылки по электронной почте. Электронный фишинг – метод, при котором рассылаются тысячи мошеннических сообщений. Ссылки внутри сообщений напоминают свои реальные аналоги, но содержат неправильное имя домена или дополнительные поддомены. После перехода по данной ссылке мошенник получает информацию, которую вводит жертва.

Направленный фишинг нацелен на конкретного человека или предприятие. Это более глубокий тип фишинга, который требует специальных знаний об организации, включая ее иерархию. Выдавая себя за высокопоставленное лицо, злоумышленник крадет учетные данные, получая полный доступ к конфиденциальным данным в сети организации.

Методы предотвращения фишинга. Для пользователей бдительность является ключевым фактором. Пользователи также должны остановиться и подумать о том, почему они вообще получают такое письмо. Двухфакторная аутентификация (2FA) является наиболее эффективным методом противодействия фишинговым атакам, поскольку она добавляет дополнительный уровень проверки при входе в чувствительные приложения. В дополнение к использованию 2FA организации должны пользоваться сложными паролями. Образовательные кампании также могут помочь уменьшить угрозу фишинговых атак, применяя безопасные методы, такие как отказ от перехода по внешним ссылкам электронной почты.