УДК 304.444

Демидов Михаил Александрович
студент 3 курса
Челябинское высшее военное авиационное училище штурманов
Россия, г. Челябинск
e-mail: miha3003000@mail.ru

Васильев Виктор Александрович
студент 3 курса
Челябинское высшее военное авиационное училище штурманов
Россия, г. Челябинск

Научный руководитель: Иванов Денис Александрович
преподаватель, капитан
Челябинское высшее военное авиационное училище штурманов
Россия, г. Челябинск

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И МЕТОДЫ БОРЬБЫ С НЕЙ

Аннотация: *В статье рассматривается понятие социальной инженерии и методы борьбы с ней. Авторы дают характеристику основных способов хищения информации, в частности, в финансовой сфере, в заключении даются рекомендации по защите своих данных.*

Ключевые слова: социальная инженерия, методы борьбы, способы хищения.

Demidov Mikhail Alexandrovich
3rd year student
Chelyabinsk Higher Military Aviation School of Navigators
Russia, Chelyabinsk

Vasiliev Victor Alexandrovich
3rd year student
Chelyabinsk Higher Military Aviation School of Navigators
Russia, Chelyabinsk

Scientific adviser: Ivanov Denis Aleksandrovich
teacher, captain
Chelyabinsk Higher Military Aviation School of Navigators
Russia, Chelyabinsk

SOCIAL ENGINEERING AND METHODS OF STRUGGLE WITH IT

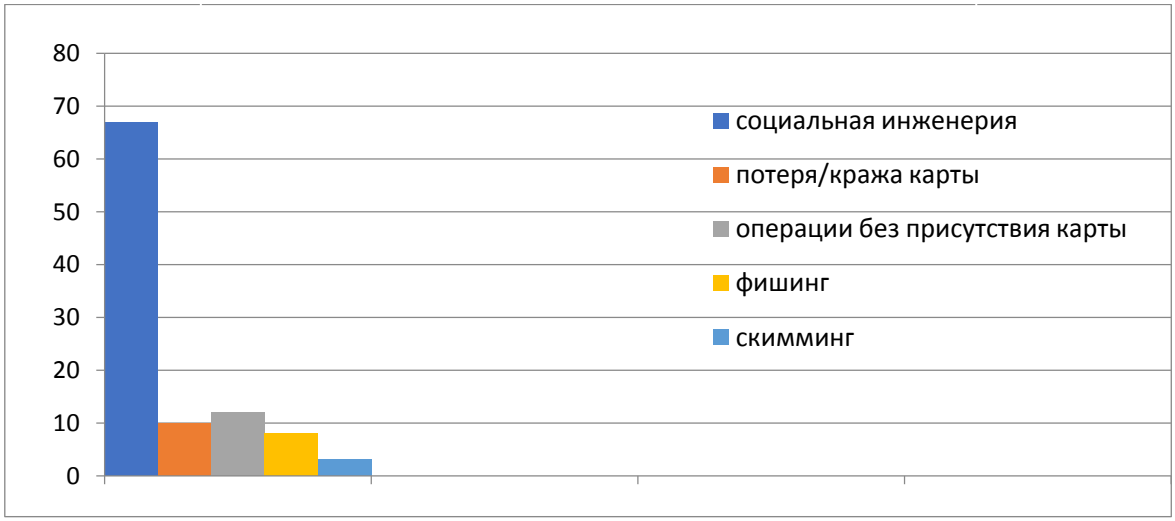
Abstract: *The article discusses the concept of social engineering and methods of dealing with it. The authors characterize the main methods of information theft, in particular, in the financial sphere; in conclusion, recommendations are given for protecting their data.*

Key words: social engineering, methods of struggle, methods of theft.

В современном мире высоких технологий способов влияния на безопасность информации становится все больше и больше. У людей (мошенников), желающих завладеть вашими данными появляются более новые способы хищения информации. Особенно это проявляется в финансовой сфере. Наиболее распространенными методами являются: скимминг, фишинг, операции без присутствия карты, потеря/кража карты, социальная инженерия.

Проведенный анализ (рис.1) по данным различных банков за 2019 год выявил, что самым широко используемым методом хищения денежных средств является социальная инженерия. Показатель данного метода составил 67 процентов, что на фоне остальных методов хищения он является наиболее популярным.

Статистика хищений данных за 2019 год



Разберём, что представляет собой социальная инженерия и как обезопасить себя от нее.

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью

социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

Типичное мошенничество такого рода выглядит следующим образом: жертве звонит преступник, представляющийся сотрудником банка. По его словам, деньги пользователя в опасности: его личный кабинет только что попытались взломать, со счета выводились средства. Служба безопасности готова спасти ситуацию при небольшом содействии самого клиента банка: к примеру, ему следует установить программу удаленного управления. После этого мошенник сам получает доступ к приложениям и выводит деньги со счета. Как правило, преступники звонят с «номеров банков», используя особые программы для изменения телефона, а также сообщают жертве некоторую персональную информацию, чтобы втереться в доверие, — такие данные можно легко купить в сети.

Связываясь с жертвой, злоумышленники вводят ее в заблуждение и выманивают банковские реквизиты и пароли. Нередко они даже напрямую просят сделать денежный перевод. Инструментов у них немало: известны случаи обмана через SMS-сообщения, социальные сети, телефонные вызовы. Дополнительной тенденцией становится установка механизма удаленного управления: грабители уговаривают загрузить на телефон определенную программу и запустить ее, и через нее полностью захватывают мобильное устройство.

Существуют ещё случаи, когда пользователям в интернете обещают крупную сумму за участие в той или иной акции или прохождение опроса. Но, чтобы получить деньги, человек сначала должен оплатить «комиссию» или «сервисный сбор» (обычно сумма небольшая, чтобы не вызвать подозрений. После этого пользователь не только не получает выигрыш, но и прощается с «комиссией», а его платежные данные оказываются в руках злоумышленников. Чаще всего мошенники притворяются крупными компаниями и банками, но бывают и случаи со знаменитостями.

Эксперты уверены, что этот популярный вид мошенничества в ближайшем будущем останется наиболее распространенным. По их словам, это связано с тем, что такой заработок стал наиболее выгодным для преступников — минимальные затраты при максимальном «доходе». При этом подозрительную активность в системах готовы отслеживать только крупные банки, что развязывает руки злоумышленникам.

На основе выше изложенного были сформированы основные методы защиты:

Нужно всегда держать в тайне следующие данные: коды из SMS и PUSH-уведомлений, PIN-код карты, контрольные вопросы, данные карты, включая срок действия и трехзначный код. Нельзя также раскрывать персональные данные: отчество, место и год рождения, данные паспорта.

Если кто-то позвонил сам, не следует ему доверять, даже если он представился сотрудником банка. Нужно перезвонить в банк в случае подозрительного звонка или сообщения от банка.

Не нужно скачивать никакие программы на смартфон по просьбе незнакомцев и тем более предоставлять им доступ к ним.

Не нужно носить записанный пин-код рядом с картой. Лучше подключить оповещения об операциях и настроить лимиты на траты.

Для быстрой связи с банком нужно заранее сохранить его номера в телефоне.

Если украли деньги со счета — нужно связаться с банком и описать ситуацию. После чего — написать заявление в полицию и отправить в банк талон о принятии заявления