УДК 004

ФИШИНГ КАК МЕТОД СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ФИНАНСОВОМ МОШЕННИЧЕСТВЕ

Миначева Э.Ф., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова*: социальная инженерия, фишинг, фишинговые атаки, мошенничество, атака.*

Атаки с использованием методов социальной инженерии являются одним из самых опасных и распространенных видов атак. В данной статье проведено исследование применения методов социальной инженерии в фишинговых атаках. Сформированы признаки отнесения интернет-ресурсов к фишинговым.

Одним из самых слабых звеньев любой системы защиты является человеческий фактор. Методы социальной инженерии позволяют злоумышленнику незаконно получить пользовательскую информацию, в дальнейшем используемую для финансового мошенничества и кражи личных данных, с минимальными временными затратами.

В настоящее время одним из наиболее распространенных методов социальной инженерии стал фишинг. Стремительное развитие Интернет-технологий дало толчок не только развитию электронной коммерции и различным онлайн-сервисам, но и электронному мошенничеству, кибератакам [1].

Первоначально под фишингом понимались сообщения электронной почты, схожие с сообщениями от легальных организаций, Интернет-ресурсов и порталов, например, страховых компаний, онлайн-магазинов, социальных сетей. В подобных сообщениях пользователю предлагается совершить какое-либо действие (например, подтвердить учетную запись), при этом пользователя мотивируют чувствами срочности или выгоды (например, блокировка учетной записи, получение подарка от компании). Дальнейшим развитием стало создание фишинговых сайтов, рассылка сообщений в популярных мессенджерах.

На фишинг, связанный с финансовым сектором, в последние годы приходится значительная доля, так в 2017 году его показатели превысили уровень в 50 % [1]. Согласно данным по спаму и фишингу в 2018 году на финансовый сектор пришлось 35,72 % фишинговых атак [2]. По

данным Центрального банка Российской Федерации [3], на 01.01.2019 в более чем 93 % открытых клиентами (физическими и юридическими лицами) в России счетов в кредитно-финансовых организациях подключена возможность получения доступа через сеть Интернет, что ставит вопрос финансового фишинга более объемным и проблемным как для клиентов, так и для организаций.

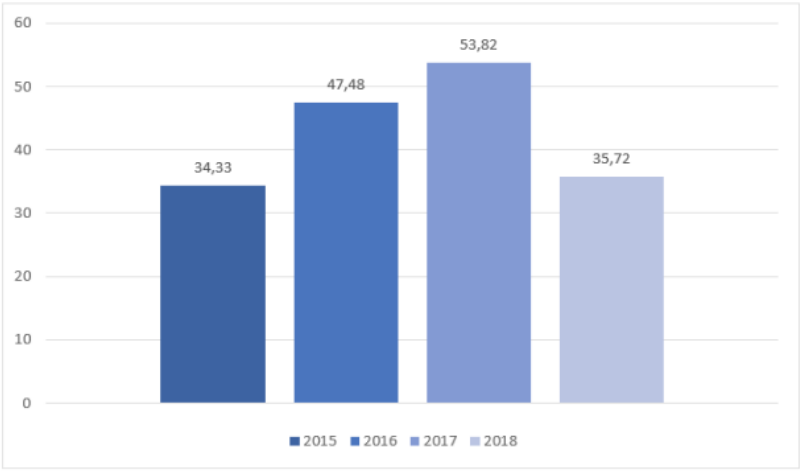

Рисунок 1 - Доля финансового фишинга в общем количестве

Фишинг можно разделить на три группы [4]:

– почтовый;

– онлайновый;

– комбинированный.

При реализации почтового фишинга злоумышленниками осуществляется рассылка почтовых сообщений, побуждающих пользователей к отправке конфиденциальных данных, например, логина и пароля. Для увеличения эффективности злоумышленниками может применяться спуфинг — подменный почтовый заголовок. Данный метод позволяет скрыть реального отправителя сообщения и выдать отправителя сообщения за существующего и вероятно знакомого пользователям, не вызывающего недоверия. Стоит отметить, что в настоящее время почтовый фишинг преимущественно применяется для доставки полезной

нагрузки, находящейся во вложении. Целью злоумышленников в подобных рассылках является создание сообщений, побуждающих пользователя открыть вложение.

Онлайновый фишинг. Зачастую Интернет-ресурсы являются подделкой официального сайта известных компаний, так называемый brand spoofing. Целью создания таких ресурсов является получение логинов и паролей, получение денежных средств под видом продажи услуг/товаров или осуществления денежных переводов, сбор данных о банковских счетах и картах. Для компаний подобный фишинг также несет репутационные риски.

Наиболее распространенные виды фишинговых Интернет-ресурсов, создаваемых и использующихся злоумышленниками в России:

- Авиабилеты;
- Магазины;
- Финансовые пирамиды;
- Кредитно-финансовые организации;
- Страховые компании.

При отнесении Интернет-ресурсов к категории фишинговых можно выделить следующие признаки:

– у организации, осуществляющей продажу товаров или оказание лицензируемых услуг, отсутствует лицензия;

– об организации, осуществляющей продажу товаров или оказание лицензируемых услуг, отсутствует информация в справочниках и реестрах уполномоченных органов государственной власти;

– при перечислении денежных средств в счет оплаты оформленного заказа платеж осуществляется в пользу третьего лица;

– название сайта/компании и/или дизайн сайта схож или полностью копирует сайт существующей организации (при этом информационный ресурс не является официальным и не имеет никакого отношения к организации).

На текущий момент почтовый фишинг не применяется в чистом виде. Поэтому применяют комбинированный. В большинстве случаев является первым этапом сложных атак с применением методов социальный инженерии. Например, комбинированный фишинг применяется в атаках по распространению банковских троянов семейства RTM и Dimnie [6].

Поскольку отдельные конфиденциальные данные физических лиц, как и инфраструктура организаций становится все более уязвимыми из-за атак, воздействующих на человеческие эмоции, возможно, приходит время для целенаправленного инвестирования в повышение

осведомленности граждан, а также работников и клиентов организаций в вопросах финансовой грамотности и информационной безопасности [7]. Безусловно, данный вопрос должен поднимать и на государственном уровне, что уже начинает происходить сейчас. Знание работника организации о том, каким образом он может стать частью сложной целевой атаки или каким атакам он может подвергнуться во время различных операций и действий в сети Интернет, положительно влияет на снижение уровня успешных фишинговых атак и увеличивает самосознание гражданами возможных последствий их действий.

Библиографический список:

1. Гуськова, А. М. Особенности инцидентов информационной безопасности в кредитно-финансовых организациях / А. М. Гуськова // Информатика и системы управления. - 2017. - С. 144–147.
2. Спам и фишинг в 2017 году // KasperskyLab. – URL : https://securelist.ru/spam-and-phishing-in-2017/88630/
3. Спам и фишинг в 2018 году // KasperskyLab. – URL : https://securelist.ru/spam-and-phishing-in-2018/93453/
4. Количество счетов с дистанционным доступом, открытых в кредитных организациях // Центральный банк Российской Федерации. – URL : http://www.cbr.ru
5. Кузнецов, И. В. Социальная инженерия и социальные хакеры / И. В. Кузнецов. – Санкт-Петербург : БХВ-Петербург, 2017. - 368 с.
6. Лаборатория Касперского зафиксировала резкий всплеск атак банковских троянцев Buhtrap и RTM // KasperskyLab. – URL : https://www.kaspersky.ru
7. Голубев, С. В. Информационная безопасность в автоматизированных системах управления / С. В. Голубев, С. А. Голубева, Е. А. Голубева // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения : материалы VIII Международной научно-практической конференции молодых ученых. – Ульяновск : УлГАУ, 2017. – С. 31-34.

PHISHING AS A SOCIAL ENGINEERING METHOD IN FINANCIAL FRAUD

Minacheva E.F.

Key words: *social engineering, phishing, phishing attacks, fraud, attack.*

Attacks using social engineering methods are one of the most dangerous and common types of attacks. This article investigates the use of social engineering methods in phishing attacks. There are signs that Internet resources are classified as phishing.