Социологические науки

УДК 004

Л.М. Гугаси

О.А. Вертиевец

Гугаси Лиана Максими, бакалавр 4 курса группы ИС-15 ФСКДТ Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: linok-linok.bk@mail.ru

Вертиевец Оксана Анатольевна, старший преподаватель кафедры экономики и информационных технологий Краснодарского государственного института культуры (Краснодар, ул. им. 40-летия Победы, 33), e-mail: magda76@mail.ru

ФИШИНГОВЫЕ АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ

В статье рассматриваются атаки, совершаемые против обычных пользователей во всемирной паутине, а также методы по борьбе с ними.

Ключевые слова: фишинг, атаки, мошенники, Интернет.

L.M. Gugasi

O.A. Vertievets

Gugasi Liana Maximi, bachelor of 4th course of IS-15 group of FSCAT of the Krasnodar state institute of culture (33, im. 40-letiya Pobedy St., Krasnodar), e-mail: linok-linok.bk@mail.ru

Vertievets Oksana Anatolyevna, senior lecturer of department of economics and information technology of the Krasnodar state шnstitute of culture (33, im. 40-letiya Pobedy St., Krasnodar), e-mail: magda76@mail.ru

PHISHING ATTACKS AND METHODS OF FIGHT WITH THEM

The article discusses the attacks committed against ordinary users on the world wide web, as well as methods of fight with them.
Key words: phishing, attacks, scammers, internet.

На настоящем этапе развития компьютерные технологии оказались естественной составляющей жизни каждого человека. Посредством гаджетов и интернета практически любой человек без всякого усилия способен получить необходимую информацию, руководить своими финансами, осуществлять разные операции.

Интернет является неограниченным пространством информации, дающим возможность коммуникации, обучения, осуществляющим реализацию работы и отдыха, каждодневно обогащающейся базой данных, хранящей в себе привлекательную для мошенников информацию о ее пользователях. Имеется два основных типа опасностей, которым подвержены пользователи: техническая и социальная инженерия. Первый тип основывается на внедрении вредоносных программ, а второй тип – это прежде всего фишинг-атаки [2].

Фишинг – переводится с английского языка как «ловить рыбу, рыбачить» – аналогия ловли рыбы, но «добычей» уже являются пользователи, их конфиденциальная информация и капитал [1].

Фишинг-атаки формируются согласно следующему принципу: мошенники разрабатывают ложный сайт, который практически невозможно отличить от настоящего сайта банка или других учреждений. Затем для получения конфиденциальных данных о пользователях нужно заманить их на данный сайт. Получив необходимую информацию, злоумышленники располагают всеми финансами пользователя и переводят их себе.

Привлечение на фиктивные сайты является довольно простой задачей. В большинстве случаев используется почтовая рассылка – это письма на вид совершенно идентичные письмам из банка или иных финансовых учреждений. Мошенники при составлении письма указывают, на первый взгляд, абсолютно правдоподобные причины, согласно которым необходимо ввести или отправить личные данные, например, для проверки учетной записи. Подобные уловки и являются приманками, благодаря которым пользователи добровольно дают информацию, которая после используется для кражи.

Одной из популярных разновидностей фишинга является массовый фишинг. Данный метод преобладает, так как он не нацелен на определенного пользователя. Здесь применяется метод социальной инженерии, направленный на большинство. При таком методе нет надобности в долгом поиске информации, мошенники отправляют сообщение от представителей известных брендов.

На сегодняшний день фишинговые атаки проводятся не только по интернету. Мошенники также отправляют письма из разных банков или учреждений с просьбой позвонить по указанному номеру для разрешения проблемы, а после звонка автоответчик просит указать личные данные. Данный метод фишинга называется «вишинг» (голосовой фишинг)

Весьма популярным также является SMS-фишинг, который еще называют «смишинг». Злоумышленники отправляют сообщения, в которых указывают ссылку на фишинговый сайт, после перехода по ссылке и ввода данных пользователь моментально становится жертвой фишинговой атаки.

Придерживаясь определенных правил, пользователи могут легко обезопасить себя. При получении подобных сообщений необходимо быть чрезвычайно осторожным, так как банки редко запрашивают подобные данные через электронную почту. При возникновении такой ситуации следует сначала позвонить в банк и уточнить, проводилась ли официальная рассылка данных сообщений. Надо также быть осторожным при заполнении

анкет на сомнительных сайтах, быть внимательнее к своим банковским счетам и выпискам. Обязательным является контроль за антивирусными программами, необходимо обратить внимание на то, чтобы антивирусная программа имела возможность блокировки подобных фишинговых сайтов [3].

Исходя из сказанного выше, можно сделать вывод, что кибер-мошенники в нынешнее время имеют довольно много способов для получения личных данных, с помощью которых могут осуществлять кражи. Задача любого пользователя – быть бдительнее при получении поступающих сообщений с незнакомых номеров, различных ссылок на незнакомые сайты.

Список используемой литературы:

1. *Джеймс Л.* Фишинг. Техника компьютерного преступления. М.: НТ Пресс, 2008. 320 с.
2. *Камский В.А.* Защита личной информации в интернете, смартфоне и компьютере. СПб.: Наука и техника, 2017. 272 с.
3. *Лямин Л.* Мошенничество в платежной сфере. Бизнес-энциклопедия / Л. Лямин, Н. Пятиизбянцев, А. Пухов, П. Ревенков. М.: Интеллектуальная Литература, 2016. 345 с.
4. *Масалков А.С.* Особенности киберпреступлений: инструменты нападения и защита информации. М.: ДМК Пресс, 2018. 226 с.
5. *Шаньгин В.* Информационная безопасность и защита информации. М.: ДМК Пресс, 2017. 702 с.