ЗАЩИТА ОТ ФИШИНГА

Никонорова Л. И.,
доцент кафедры математики, физики и информационных технологий
ФГБОУ ВО Мичуринский ГАУ,
г. Мичуринск, РФ.
Lenaniknrva@rambler.ru
Бабайцев А. В.,
студент 1 курса инженерного института
ФГБОУ ВО Мичуриский ГАУ,
г. Мичуринск, РФ.
dre.babaitsev@icloud.com
Шацкий В. А.,
студент 1 курса инженерного института
ФГБОУ ВО Мичуриский ГАУ,
г. Мичуринск, РФ.
shatskiy2000@list.ru

Анатация. Проблема защиты от фишинга и фишинговых атак в интернете.

Ключевые слова. Защита, фишинг, персональные данные.

Одним из самых популярных методов мошенничества в интернете является – Фишинг Слово «фишинг» напрямую заимствовано из английского языка. «*Fishing*» – рыбалка.

С помощью поддельных сайтов, электронных писем, телефонных номеров злоумышленники получают доступ к персональной информации человека, такой как: номера карточек, логины и пароли, контактная информация, что приводит к получению доступа к счетам и личным данным пользователей. В ряде случаев, используется массовая рассылка от лица

популярных сайтов, компаний, организаций, которые содержат ссылки на ненастоящие сайты, внешне неотличимые от своего оригинала. На данных «сайтах-приманках» пользователя просят указать свои персональные данные.

Проблема состоит в том, что пользователи привыкают доверять сервисам, которыми пользуются постоянно, не задумываясь, вводят логины и пароли или платёжные информации карточки.

Одним из популярных методов фишинга является продажа фальшивых авиабилетов. Человек, купивший билет, получает письмо с квитанцией об оплате, и даже сам билет, но в аэропорту выясняется, что полететь по нему никуда нельзя.

Известными фишинговыми атаками являются: ZeuS, Dropbox, Dyre.

В конце октября 2014-го года, пользователи получали фишинговые письма с взломанного домена «edu». Такие письма содержали троян ZeuS в архиве с информацией о совершенных платежах, которых на самом деле вовсе не было. Мошенники надеялись, что домен «edu», созданный специально для образовательных учреждений, просто не покажется жертвам подозрительным. Такой способ распространения вредоносных программ и воровства данных оказался очень эффективным.

Рост популярности облачных сервисов, таких как Dropbox, позволил мошенникам создать новый метод доставки вирусного ПО в компьютеры. Мошенники отправляют по email письма с инвойсом от Dropbox. Ссылка на сервис является абсолютно чистой, только она ведет на zip-файл, содержащий файл типа SCR (зараженный скрипт), а не на счета. Dropbox быстро создал защиту для пользователей, но хакеры нашли способ обхода разработанного компанией спам-фильтра. Использование Dropbox настолько распространено, что блокировать этот сервис как потенциально опасный никому и в голову не придет, поэтому пресечь такой вид распространение вирусов и троянов крайне сложно.

Популярные фишинг-письма 2014 года приходили со ссылками на сторонние хранилища файлов. Содержание было простым – ссылка на счет,

скачивая который себе на компьютер, пользователь пускал в систему программу Dyre, троян для удаленного доступа, который был нацелен на получение банковской информации и личных данных пользователя. Распространение Dyre было широким и группе реагирования на нарушения компьютерной безопасности в сети пришлось усердно работать над тем, чтобы избавиться от этого вируса.

В настоящее время универсальной защиты от фишинга не существует, но соблюдение некоторых правил позволит предостеречь свои персональные данные от кражи.

1. Первое – это бдительность (требуется внимательно проверять ссылку сайта, на котором вы находитесь: не перепутаны ли буквы в названии сайта). Необходимо обращать внимание на защищенность соединения. Если перед адресом сайта находится префикс https (где “s” означает secure – безопасное). Даже если письмо пришло ссылкой, например, от лучшего друга, то не стоит забывать, что его тоже могли взломать.

2. Вместо того чтобы кликать по ссылке, гораздо надежнее ввести адрес вручную в новом окне браузера.

3. Вложения электронных писем так же могут содержать вредоносные программы в виде троянов. Бороться с ними вам помогут антивирусы на ПК.

4. Современные браузеры могут, помочь не попасться на мошенников, просто не пропуская на вредоносные сайты, предупреждая об опасности.

Список использованных источников

1. https://ru.wikipedia.org/wiki/Фишинг
2. https://yandex.ru/promo/safesearch/fishing
3. https://www.avast.ru/c-phishing

PHISHING PROTECTION

Nikonorova L. I.,
Associate Professor of the Department

mathematics, physics and information technology
Michurinsk State Agrarian University,
Michurinsk, Russia.
Lenaniknrva@rambler.ru
Babaytsev A. V.,
1st year student at an engineering institute
Michurinsk State Agrarian University,
Michurinsk, Russia.
dre.babaitsev@icloud.com
Shatsky V. A.,
1st year student at an engineering institute
Michurinsk State Agrarian University,
Michurinsk, Russia.
shatskiy2000@list.ru

Annotation. The article is devoted to the problem of protection against phishing and phishing attacks on the Internet, with the aim of conforming the personal and payment data of the user.

Keywords. Phishing protection. Personal Information.