УДК 004.056.5 **Информационные технологии**

Юсупов Магомед Юсупович, *студент, Московский университет МВД России имени В.Я. Кикотя*

Путилов Артур Олегович, *старший преподаватель кафедры информатики и математики Московский университет МВД России имени В.Я. Кикотя*

ФИШИНГ КАК УГРОЗА КОНФИДЕНЦИАЛЬНОСТИ В СЕТИ

Аннотация: Научная статья посвящена анализу одному из видов интернет мошенничества, которое представляет собой незаконное получение идентификационных данных пользователя, то есть пароли и логины от банковских карт или учётных записей, а также методам борьбы с фишингом. При помощи практического применения отдельных технологий и методов проведена разработка механизмов совершенствования борьбы с данными махинациями в интернете. Проведенное исследование позволяет утверждать, что бдительность пользователя сети бывает на недостаточном уровне, что приводит к неприятным последствиям. Актуальность исследования заключается в том, что во время пандемии коронавируса количество краж с банковских карт выросло в шесть раз. По словам экспертов в этой области, злоумышленники завлекают пользователей на фишинговые сайты, где те вводят свои данные, после чего мошенники переводят денег на свои счета. Один банк в среднем фиксирует 400-600 попыток такого способа мошенничества в месяц. Средний чек одного перевода — 7 тысяч рублей. В 2021 году — от его последствий пострадали свыше 100 тысяч человек, потеряв свыше $57 млн.[2].

Ключевые слова: Фишинг, защита данных, уязвимость в интернете, кибербезопасность, цифровые технологии, личные данные, киберпреступники.

Annotation: The scientific article is devoted to the analysis of one of the types

of Internet fraud, which is the illegal obtaining of user identification data, that is, passwords and logins from bank cards or accounts, as well as methods of combating phishing. With the help of the practical application of certain technologies and methods, mechanisms have been developed to improve the fight against these frauds on the Internet. The conducted research allows us to assert that the vigilance of the network user is at an insufficient level, which leads to unpleasant consequences. The relevance of the study is that during the coronavirus pandemic, the number of thefts from bank cards increased sixfold. According to experts in this field, cybercriminals lure users to phishing sites, where they enter their data, after which the scammers transfer money to their accounts. One bank, on average, records 400-600 attempts of this type of fraud per month. The average bill of one transfer is 7 thousand rubles. In 2021 - over 100 thousand people suffered from its consequences, having lost over $ 57 million [2].

Key words: Phishing, data protection, internet vulnerability, cybersecurity, digital technology, personal data, cybercriminals.

Современный период трансформации мировой и отечественной экономики способствует усилению интеграционных процессов между коммерческой деятельностью и цифровыми технологиями, последние из которых выступают главным фактором стремительного развития бизнес-субъектов в интернете, из-за чего злоумышленникам, а точнее киберпреступникам стало легче получить нужную им информацию. Каждый из нас уязвим в сети, все зависит от нашей внимательности. Для того, чтобы понимать, о чем идет речь в данной статье, нужно понять, что же значит «Фишинг». Чаще всего он представляет собой какие-то массовые рассылки писем или уведомлений на почты от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей, доверие к которым однозначно заложено в мышлении пользователя сети. В письме из рассылки часто содержится прямая ссылка на сайт который сложно отличить от оригинального. Фишинговые атаки могут быть направлены как на частных

лиц, так и на отдельные компании. Так, к примеру, главе избирательного штаба Хилори Клинтон, Джону Подеста, хакеры прислали предупреждение, что пароль к его почтовому ящику на Google был взломан и его рекомендуется сменить. Джон перешел по указанной ссылке и сменил свой пароль на поддельном сайте, таким образом передав доступ к своей почте злоумышленникам. Как результат, в интернет попали десятки тысяч его электронных писем, многие из них оказались компрометирующими. Рейтинг Хилори Клинтон упал и в итоге она проиграла выборы Дональду Трампу.

Исследование актуально по причине увеличения массовой доли преступлений, совершенных в сети Интернет, в общей массе преступлений, совершенных в Российской Федерации.

Актуальность фишинга и конфиденциальности информации требует внимательного отношения к задаче ее защиты. 20 лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно, любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры.

Постановкой научной проблемы выступает низкий уровень обеспечения информационной безопасности в интернете, который приводит к возможным негативным последствиям, среди которых потеря конфиденциальной информации и кража персональных данных конкретных лиц, а также групп лиц. По нашему мнению, в случае отсутствия активного исследования на тематику «фишинг как угроза конфиденциальности в сети», мы способны столкнутся с ситуацией, при которой, безопасность общества и отдельных индивидуумов будет под угрозой. При этом, в настоящее время фишинг является актуальной проблематикой и для корпоративных/предпринимательских структур, коммерческая информация и интеллектуальный капитал которых находится в поле поиска злоумышленников.

По этой причине, целью научной статьи выступает анализ фишинга как угрозы конфиденциальности личной информации в сети Интернет. Необходимо узнать, с какой целью происходит получение ценных данных пользователей, которые могут быть проданы или использованы нарушителями закона.

Рассмотрим ещё несколько примеров, к вам на почту приходит письмо с тем, что якобы в ваш профиль зашли с неизвестного устройства, необходимо незамедлительно перейти по ссылке, чтобы вернуть ваш аккаунт. Пользователь не задумываясь переходит, вводит свои данные, даже не обратив внимания по какой ссылке он перешел. К сожалению, практически никто не обращает своего внимания на адрес страницы, открывающейся в браузере, в результате жертвы добровольно передают все свои данные мошеннику, но и это не все беды, которые может принести фишинговая ссылка. Через такую ссылку также можно получить: Вирус-шпион, Кейлоггер или даже троян. Так, злоумышленники получат доступ не к одному вашему аккаунту, а ко всем сразу. Не обнаружив вовремя угрозу, вы будете сами долгое время передавать все свои персональные данные.

К основным методикам и техникам фишинга относят [3]:

1) Приёмы социальной инженерии

Хакеры хотят вывести цель на эмоции, выдавая себя за представителей известной компании, сообщая о том, что необходимо внести новые персональные данные клиента из-за утери данных, программного сбоя и др.

2) Фишинг с обманом

В данном случае мошенник отправляет на почту письмо от имени организации с просьбой перейти по ссылки для того, чтобы подтвердить (проверить) в учётной записи свои данные. Для этого создаются фишинговые сайты в точности схожие с оригинальными, чтобы пользователь не смог сразу догадаться о махинации.

3) «Гарпунный» фишинг

Целью «Гарпунного фишинга» становятся отдельные личности. Хакеры узнают практически все о своих жертвах, для этого они прибегают к

социальной инженерии и к другим сервисам, в которых содержится хоть какая-то информация об объекте.

4) Рассылка вирусов

Случается, что злоумышленники желают не украсть какую-то информацию, а нанести ущерб отдельным личностям или группам лиц. Ссылка, которую прислали на почту, может загружать на ПК вредоносные вирусы.

5) Фарминг

Мошенники пользуются именно официальными сайтами. Фармеры меняют цифровой адрес оригинального сайта на DNS-сервере на адрес подменного сайта, в результате человек, зайдя желаемый сайт, переходит на поддельный.

6) Вишинг

Способ фишинга, использующий мобильную связь. В письме указывается телефонный номер, на который вам нужно перехвонить, для устранения «Возникших проблем», затем мошенник просит указать персональные данные, например, для входа в банк.

Проблема настолько серьезная, что ее предлагают внести как статью в уголовный кодекс РФ:

Российских кибермошенников, которых уличат в создании фишинговых сайтов, будут сажать в тюрьму на срок до четырёх лет, если Госдума примет законопроект, который начинают разрабатывать по инициативе члена комитета по безопасности и противодействию коррупции Ильи Костунова. Он предложил ввести уголовную ответственность за создание фишинговых сайтов и владение ими.

Фишинговые сайты используются для сбора информации у пользователей интернета. Например, это могут быть поддельные банковские сайты или клоны Вконтакте, которые внешне копируют оригинал. Здесь пользователю предлагают ввести логин и пароль. Учётные данные сохраняются, а пользователя перенаправляют на оригинальный сайт с пройденной авторизацией. Таким образом, жертва ничего не замечает.

Депутат предлагает разработать законопроект, вводящий механизм досудебной блокировки фишинговых сайтов, похожих до степени смешения на существующие популярные сайты и незаконно собирающих персональные данные или платёжную информацию пользователей. Механизм блокировки прорабатывается: возможно, на сайте Роскомнадзора появится форма для сбора информации о фишинговых сайтах. Или правообладатель обратится в суд и уже затем передаст Роскомнадзору список адресов для блокировки.

Ну, а владельцам таких сайтов грозит уголовная ответственность. Сейчас за фишинг в УК РФ ответственность не предусмотрена. Поэтому предлагается дополнить главу 28 УК РФ «Преступления в сфере компьютерной информации» новой статьёй, включающей ответственность за создание и владение фишинговыми сайтами. По мнению депутата, за это преступление следует брать большой штраф либо лишать свободы на срок до четырёх лет.

Разберем на примере сайта Google, как работают фишинговые сайты:

1) Создаются абсолютно идентичные страницы того сервиса, данные которой нужны хакеру (Дизайн, расположение ввода данных и т.д.);

2) Сайт загружается на хостинг и ему присваивается доменное имя;

3) Злоумышленники меняют название сайта так, чтобы оно было минимально отличимо от оригинала (Меняют точку на тире и наоборот, заменяют похожими в произношении буквами, перед настоящим названием сайта присваивают «Help», «Login» и так далее.);

4) Теперь создается шаблон для рассылки и в него встраивается ссылка на фишинговый сайт, она может быть как прямой, так и скрытой (Название сайта вроде правильное, но URL ссылка совершенно другая).

Злоумышленники довольно часто маскируют ссылки различными способами, одним из способов является сокращение ссылки. Сам процесс сокращения ссылки заключается в использовании специального сервиса, который генерирует короткий код для доступа к блоку, в котором хранится первоначальная ссылка, при переходе по этому коду сервер находит адрес у

себя в базе и перенаправляет запрос. Ссылка сокращается посредством изменения числа символов, или же присвоения ссылки какого-то определенного слова.

Как же проверить что скрывается за ссылкой, которую хакеры сократили? Достаточно добавить в поисковой строке после самой ссылки слово «info».

Стоит отметить статистику фишинга за 2020-2021:

- «Лаборатория Касперского» выявила 184 435 643 вредоносных вложения.
- «Антифишинг» предотвратил 434 898 635 попыток мошенников получить данные.
- Самая частая цель злоумышленников – Онлайн магазины, а именно 18,12% атак были направлены в их сторону
- Топ 5 наиболее подверженных фишинговым атакам сайты: Google и Amazon – по 13%, WhatsApp и Facebook – по 9%, Microsoft – 7%.
- В связи с вирусом COVID-19, около 13% фишинговых атак были основаны на теме пандемии, из них 44% на частные лица.
- Более 34% всех атак на юридические лица содержали в себе троянов шифровальщиков
- .График статистики попыток фишинговых атак:

6 апреля 2021 года стало известно о выявлении в России 1529 лжебанков по итогам первого квартала. Это на 20% больше по сравнению с первыми тремя месяцами 2020-го. Об этом свидетельствуют данные компании BI.ZONE, специализирующейся на технологиях обеспечения информационной безопасности.

Мошенники маскируются под настоящие кредитные организации и обманом заставляют своих жертв вводить логины и пароли от своих реальных банковских аккаунтов или вносить предварительную комиссию для получения услуги по заниженной цене. Чтобы обезопасить себя, злоумышленники зачастую копируют фирменный стиль банка, и меняют одну-две буквы в юридическом названии.

Гуськова А. М. в своей работе рассматривает фишинг как основной метод социальной инженерии в схемах финансового мошенничества, также она делает вывод о том, что атаки с использованием методов социальной инженерии на текущий момент являются одним из самых опасных и распространенных видов атак, нацеленных на нарушение конфиденциальности и получения доступа, поскольку технически они ориентированы на психологические манипуляции [2].

Тумбинская М.В. описывает, что ключевой причиной информационной небезопасности пользователей социальных сетей является таргетированная информация, вызывающая информационные атаки на мнение людей [5].

Михаил Терешков, руководитель направления информационной безопасности АО «ЭР-Телеком Холдинг», в колонке на Rusbase привел такие эффективные, но простые для пользователя способы защиты от фишинга [4]:

1) Смотрите на сертификат безопасности платежной системы — в адресной строке браузера название сайта выглядит как https://...

2) Всегда изменяйте установленные заводские пароли роутера на более сложные, а также минимум раз в полгода устанавливайте обновленные версии ПО.

3) Не приобретайте какой-либо товар через общественный Wi-Fi.

Дополнительной защитой может стать антивирус для смартфона.

4) Прежде чем осуществлять оплату в незнакомом интернет-магазине, почитайте о нем отзывы в сети.

Еще немного советов от «Касперского»:

1. Перед тем как пройти по ссылке, проверьте правильность чередования букв. Если буквы поменялись местами, это явный признак того что ссылка фишинговая.

2. Проверьте, защищено ли соединение, перед тем как вводить данные. Если перед адресом сайта вы увидите префикс https (где «s» означает secure — безопасное), то все в порядке.

3. Не стоит обращать внимание на то, что отправитель ваш знакомый или близкий человек, ведь и его могли взломать. Поэтому ведите себя не менее осторожно, чем при обращении со ссылками, пришедшими из неизвестного источника.

4. Нужно проверять сообщения даже из официальных источников: сеть, магазинов, работа. Злоумышленникам не так сложно подделать официальное письмо так, что вы не увидите разницы.

5. Иногда подделанные сообщения и ненастоящие сайты во всем копируются с оригинальных. А вот гиперссылки, скорее всего, будут некорректными — или с переадресацией, или вообще не будут работать. По этим свойствам можно отличить поддельное письмо от настоящего.

6. Гораздо лучше, если вы введете адрес ссылки вручную, так вы не попадетесь на удочку «Фишеров».

7. Если вдруг вы обнаружили фишинговое письмо из банка, лучше незамедлительно сообщить об этом в саму организацию, чтобы в дальнейшем предотвратить обман людей хакерами.

8. Не стоит заходить в мобильный банк используя Wi-Fi сеть в интернет кафе и других местах скопления людей. Дело в том, что за таким Wi-Fi могут стоять злоумышленники, меняющие адрес сайта на уровне подключения и перенаправляющие вас таким образом на поддельную страницу.

9. Файл, который вам прислал ваш товарищ по игре, может оказаться трояном-шпионом или даже трояном-вымогателем, как и вложения к письмам и сообщениям. Будьте бдительны!

Библиографический список:

1. Компания Group-IB: https://www.group-ib.ru/.

2. Гуськова А.М. Фишинг как основной метод социальной инженерии в схемах финансового мошенничества // 3 международная научная конференция Исследования молодых учёных. 2019.

3. Кузнецов А. Что такое фишинг и как от него защититься URL: https://rb.ru/story/what-is-fishing/.

4. Терешков М. «Вариантов стать жертвой мошенников — масса». Как защитить себя от злоумышленников в сети? URL: https://rb.ru/opinion/zashiti-sebya-ot-moshennikov/.

5. Тумбинская М.В. Обеспечение защиты от нежелательной информации в социальных сетях // Вестник МГУ. 2017. №2.