УДК 004.056.5

ФИШИНГОВЫЕ АТАКИ КАК УГРОЗА БЕЗОПАСНОСТИ ЛИЧНОСТИ В ИНТЕРНЕТЕ

Клейменкин Д.В.
магистрант,
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,
Шахты, Россия
Могилевская Г.И.
доцент, кандидат философских наук,
Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,
Шахты, Россия

Аннотация
Статья посвящена проблеме противодействия фишинговым атакам, так как они могут стать способом кражи личной информации. Есть множество фильтров от спама, но фишинговые письма могут выглядеть обманчиво правдоподобными. Некоторые из них даже персонализированы для конкретного пользователя. По всему Интернету фишинговые атаки заставляют ничего не подозревающих жертв передавать банковскую информацию, номера социального страхования и многое другое. В этой статье будет рассмотрено влияние таких фишинговых атак на нарушение приватной сферы пользователей интернета.
Ключевые слова: фишинговые атаки, онлайн-мошенничество, безопасность личности в Интернете, приватность человека.

AUTOMATIC SEGMENTATION OF SATELLITE IMAGES BASED ON A CONVOLUTIONAL NEURAL NETWORK

Kleimenkin D.V.
master's student,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia
Mogilevskaya G.I.
docent, Candidate of Philosophical Sciences
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia

Abstract
The article is devoted to the problem of countering phishing attacks, as they can become a way of stealing personal information. There are plenty of spam filters, but phishing emails can look deceptively plausible. Some of them are even personalized for a specific user. All over the internet, phishing attacks force unsuspecting victims to hand over banking information, social security numbers, and more. This article will examine the impact of such phishing attacks on the violation of the privacy of Internet users.
Keywords: phishing attacks, online fraud, personal security on the Internet, social privacy of a person.

На сегодняшний день в России начинает увеличиваться рост преступлений с помощью информационных технологий. Фишинг-атаки можно назвать преступлением XXI века. Фишинговые атаки преследуют как частные лица, так и организации с момента изобретения электронной почты, со временем становясь всё более изощренными и замаскированными. Фишинговая атака – один из распространенных способов, используемых злоумышленниками для проникновения в учетные записи и сети своих жертв. Интернет – это безграничный мир информации, который дает широкие возможности для

общения, обучения, организации работы и отдыха, но в то же время представляет собой огромную, ежедневно пополняющуюся базу данных. Другими словами, эти схемы социальной инженерии «заманивают» доверием, чтобы получить ценную информацию. Это может быть что угодно – от входа в социальную сеть до выявления всех личностных данных через номер социального страхования. Эти схемы могут побудить перейти по ссылке, открыть вложение или раскрыть личную информацию [1].

Наиболее распространенные сценарии заключаются в следующем:

1. При открытии электронной почты внезапно появляется уведомление от банка. Нажимая на ссылку в электронном письме, происходит переход на веб-страницу, которая более или менее похожа на банк.

2. Этот сайт предназначен для кражи личной информации. В предупреждении будет указано, что с учетной записью возникли проблемы и будет предложено подтвердить свой логин и пароль.

3. После ввода учетных данных на открывшейся странице обычно отправляют в реальное учреждение для повторного ввода вашей информации. Направляя пользователя в законное учреждение, он не сразу понимает, что информация была украдена.

Эти угрозы могут быть очень опасными, так как угроза, исходящая от фишинга состоит в том, что он может обмануть любого, кто не скептически относится к мелким деталям.

Любой, кто пользуется интернетом или телефонами может стать мишенью для фишинговых мошенников [2].

Фишинговые мошенники обычно пытаются:

1. Заразить устройства вредоносными программами.

2. Украсть личные учетные данные, чтобы получить деньги или идентификационные данные.

3. Получить контроль над своими онлайн-аккаунтами.

4. Убедить пользователя добровольно отправлять деньги или ценности.

Иногда эти угрозы касаются не только конкретного пользователя. Если злоумышленник проникает в электронную почту, список контактов или социальные сети, он может рассылать знакомым фишинговые сообщения, предположительно от пользователя.

Также существуют распространенные типы фишинговых атак на предприятия, к ним относят такие приемы как олицетворение компании, фишинг-копье, захват учетной записи электронной почты, фишинговые письма [3].

Олицетворение компании.

Одна из наиболее распространенных форм фишинга - это когда злоумышленники выдают себя за ваш бренд. Обычно это делается с помощью электронной почты, подключенной к домену, очень похожему на целевую компанию. Компаниям также трудно остерегаться этой атаки из-за того факта, что она не узнаете об этом, пока кто-нибудь не воспользуется данным сервисом.

Фишинг-копье.

Этот тип схемы предполагает использование поддельного названия компании, а также ключевых сведений о цели. Как и в случае с продажами, представитель находит имя, должность и другие параметры персонализации и включает их в рекламное электронное письмо. Злоумышленники находят те же токены и используют их, чтобы заманить в свою ловушку больше жертв. Это особенно опасная уловка.

Захват учетной записи электронной почты.

Все члены исполнительной и управленческой команды уязвимы. Если фишинговый мошенник получает учетные данные электронной почты высокопоставленного руководства, вполне вероятно, что он нацелится на любого, кого сможет, используя именно этот адрес электронной почты. Потенциальными целями могут быть: коллеги, члены команды и даже клиенты.

Фишинговые письма

Аналогично мошенничеству с захватом учетной записи электронной почты, эта фишинговая атака осуществляется по электронной почте. Разница в том, что фишинговый мошенник использует адрес электронной почты, похожий на законный адрес электронной почты, человека или компании. Электронное письмо будет содержать запрос на переход по ссылке, смену пароля, отправку платежа, отправку конфиденциальной информации или открытие вложения файла.

Фишинг по телефону или голосовой фишинг.

Используя технологию передачи голоса по интернет-протоколу (VoIP), мошенники, опять же, выдают себя за компании. Этот метод также использует другие виды фишинга, включая использование личных данных о целях и выдачу себя за отдельных сотрудников компании (например, генерального директора), чтобы получить более высокую оценку общей аферы.

Фишинг наносит непоправимый ущерб брендам.

Хотя большинство людей согласны с тем, что фишинговые атаки и утечки данных могут повлиять на прибыль организации, они могут привести к гораздо большему, чем просто первоначальные финансовые потери.

Эти атаки обычно обнаруживаются слишком поздно. Иногда атаку обнаруживают клиенты, а не компания. В подобных случаях клиенты переносят свой бизнес в другое место из страха, что их личные данные могут быть раскрыты.

Как только информация об атаке появляется в новостях и социальных сетях, имидж бренда немедленно страдает. Читатели начинают беспокоиться о том, что вести бизнес с организацией небезопасно, и этот страх приводит к тому, что клиенты теряют доверие и даже отказываются от поврежденного бренда в пользу конкурента, который кажется гораздо более безопасным.

Клиенты могут подать иски, или организации могут быть оштрафованы за несоблюдение правил защиты данных, если они применяются.

Человеческая природа считается одним из наиболее влияющих факторов в процессе фишинга [4]. Каждый человек подвержен фишинговым атакам, потому что фишеры играют на специфических психологических и эмоциональных триггерах человека, а также на технических уязвимостях. Хотя фишингу подвержены все, исследования показали, что разные возрастные группы более восприимчивы к определенным приманкам, чем другие. Например, участники в возрасте от 18 до 25 лет более подвержены фишингу, чем другие возрастные группы. Причина, по которой молодые люди с большей вероятностью попадаются на фишинг, заключается в том, что молодые люди более доверчивы, когда дело доходит до онлайн-общения, а также с большей вероятностью нажимают на незапрашиваемые электронные письма.

Участники с высоким уровнем использования персональных компьютеров как правило, выявляют попытки фишинга более точно и быстрее, чем другие участники, а интернет-зависимость, повышенное внимание и двигательная импульсивность являются значительными положительными предикторами рискованного поведения в области кибербезопасности. Те, кто обладает большими знаниями о фишинге, более восприимчивы к фишинговым мошенничествам. Во-первых, осведомленность пользователей о фишинге, возможно, повысилась из-за постоянного попадания в фишинговые мошенничества. Во-вторых, пользователи, которые попались на фишинг, могут иметь меньше знаний о фишинге, чем они утверждают.

Методы использования паролей для обеспечения безопасности от фишинга [5]:

1. Использование уникального случайного пароля, состоящего более чем из 16 символов для каждой учетной записи.

2. Использование прописных и строчных букв, цифр и символов.

3. Управление паролями с помощью облачного менеджера паролей, такого как LastPass, OnePass или другие.

4. Изменение всех паролей не реже одного раза в год.

5. Внедрение 2-факторной аутентификации (2FA) для всех сайтов, которые ее предлагают.

Подводя итоги сказанному, можно отметить, что фишинговые атаки на сегодняшний день являются серьезной угрозой для безопасности частных лиц и организаций. Это обусловлено вовлечением человека в цикл фишинга, так как именно человеческие слабости создают условия для успешных фишинговых атак. Восприимчивость к фишингу обусловлена возрастными особенностями, половой принадлежностью, стрессовым состоянием пользователей, что требует от разработчиков компьютерных программ с целью их безопасного использования учитывать эти факторы.

Библиографический список

1. All About Phishing Scams & Prevention: What You Need to Know [Электронный ресурс] – Режим доступа – URL: https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips (Дата обращения 30.10.2022)

2. Personal Security: How to Eliminate the Internet's Info on You [Электронный ресурс] – Режим доступа – URL: https://www.greycampus.com/blog/information-security/personal-security-how-to-eliminate-the-internets-info-on-you (Дата обращения 31.10.2022)

3. Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2022 [Электронный ресурс] – Режим доступа – URL: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams (Дата обращения 01.11.2022)

4. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy [Электронный ресурс] – Режим доступа – URL: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full (Дата обращения 01.11.2022)

5. An In-Depth Guide to Personal Cybersecurity [Электронный ресурс] – Режим доступа – URL: https://medium.com/@nickrosener/an-in-depth-guide-to-personal-cybersecurity-be98ba47c968 (Дата обращения 02.11.2022)

Оригинальность 94%