С.И. Богданов – доцент, доктор медицинских наук.

Information about the authors

N.S. Zhenikhova – student

D.M. Gambaryan – student

S.E. Eseva – cardiologist

A.A. Karchava – IT-specialist

S.I. Bogdanov – Doctor of Medicine, Associate professor

УДК: 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЯ: ФИШИНГ

Кузнецова А.В.¹, Богданов С.И.²

¹⁻² ФГБОУ ВО «Уральский государственный медицинский университет»

Минздрава России, Екатеринбург, Российская Федерация

¹sasha_kuz16@mail.ru

Аннотация

Широкое распространение цифровых технологий несет в себе скрытые и явные опасности. Это напрямую связано и со здравоохранением. Одним из видов кражи информации является фишинг. В настоящее время тема фишинга коснулась практически всех сфер нашей жизни, в том числе и медицинской. В современной медицине используются новейшие достижения науки в области информационных технологий, не говоря уже о том, что медицинские организации имеют свои сайты, сотрудники пользуются электронной почтой, социальными сетями. Пациенты получают результаты медицинских исследований на свою почту, обращаются на сайты медицинских организаций. Поэтому все они могут быть подвергнуты фишинговым атакам со стороны хакеров. Врачам необходимо изучать вопросы информационной безопасности, прежде всего в связи с сохранением врачебной тайны. **Введение.** Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. **Цель исследования** - изучить виды фишинговых атак и варианты защиты от них в здравоохранении. **Материалы и методы.** В основу исследования легли материалы статьи и видеоматериалы, рассматривающие фишинговые атаки на пользователей. **Результаты.** Были проанализированы варианты фишинговых атак на примерах. Первый вариант - это переход по ссылке.

Второй вариант - это отправить вас на какой-то сайт, который очень похож на известный вам сайт, например, корпоративный портал. Третий вариант - это заставить вас запустить нечто, что прислали вам уже в письме. **Обсуждение.** В ходе исследования были проанализированы особенности фишинговых атак, их разновидности. **Выводы.** Фишинговая стратегия имеет опасность с точки зрения защиты личных данных пациентов и медицинских учреждений. Для пользователей во избежание фишинговых атак необходимо предпринимать определённые шаги.

Ключевые слова: информационная безопасность, фишинг, хакерская атака.

INFORMATION SECURITY OF A USER: FISHING

Kuznetcova A.V.¹, Bogdanov S.I.²

¹Ural state medical university, Yekaterinburg, Russian Federation

¹sasha_kuz16@mail.ru

Abstract

The widespread use of digital technologies carries hidden and obvious dangers. This is directly related to healthcare. Phishing is one type of information theft. Currently, the topic of phishing has touched almost all areas of our lives, including medical ones. In modern medicine, the latest achievements of science in the field of information technology are used, not to mention the fact that medical organizations have their own websites, employees use e-mail, social networks. Patients receive the results of medical examinations in their mail, refer to the websites of medical organizations. Therefore, all of them can be subjected to phishing attacks by hackers. The doctor needs to study the issues of information security, primarily in connection with the preservation of medical secrecy.

Introduction. Phishing (English phishing, from fishing - fishing, fishing) is a type of Internet fraud, the purpose of which is to obtain user identification data. **The aim of the study** - to study the types of phishing attacks and options for protecting against them in healthcare. **Materials and methods.** The study was based on the materials of the article and video materials that consider phishing attacks on users. **Results.** Variants of phishing attacks were analyzed using examples. The first option is to follow the link.

The second option is to send you to some site that is very similar to a site you know, such as a company portal. The third option is to have you run something that has already been sent to you in the email. **Discussion.** In the course of the study, the features of phishing attacks and their varieties were analyzed. **Findings.** The phishing strategy is dangerous in terms of protecting the personal data of patients and medical institutions. Users need to take certain steps to avoid phishing attacks.

Key words: Information Security, fishing, attack, hacker attack.

ВВЕДЕНИЕ

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей [1].

Фишинговая атака всегда нацелена на эксплуатацию какой-то слабости человека, на его невнимательность или ещё что-то, чтобы человек выполнил какие-то действия. Рассмотрим основные варианты фишинга.

Знание правил работы в сети Интернет помогут пользователям решить проблему фишинговых атак.

Цель исследования - изучить виды фишинговых атак и варианты защиты от них в здравоохранении.

МАТЕРИАЛЫ И МЕТОДЫ

В основу исследования легли материалы статьи и видеоматериалы, рассматривающие фишинговые атаки на пользователей.

РЕЗУЛЬТАТЫ

Были проанализированы варианты фишинговых атак на примерах.

Первый вариант - это переход по ссылке. Например, вам приходит письмо, и в этом письме вам предлагается перейти по некоторой ссылке. Например, вместо сайта innopolis.ru в письме может быть написано immpopolis.ru, то есть поставлена другая буква и беглым взглядом эти слова очень похожи.

При переходе по ссылке может возникнуть несколько развитий ситуации. Например, эта ссылка уже является вредоносной. На том сайте, куда вы перейдете, существует уже какой-то вредоносный код, который исполняет ваш браузер. То есть ваш браузер попытается исполнить этот код, выйдет в некоторое нестандартное состояние, и этим браузером можно будет управлять извне. Это особый раздел информационной безопасности, который называется эксплойты - это некие программные коды, которые позволяют вывести программное обеспечение в нештатную ситуацию.

Очень важно как можно чаще обновлять свою операционную систему, обновлять свой браузер, разработчики обычно об этом сообщают обязательно. Как только появилось какое-то обновление, начинается отчёт тех пользователей, которые не поставили это обновление. А соответственно хакеры, зная, что появилось обновление, внимательно изучают его, понимают, что есть какая-то уязвимость и пытаются эту уязвимость эксплуатировать на тех пользователях, которые ещё не успели обновить свою операционную систему [2].

Второй вариант - это отправить вас на какой-то сайт, который очень похож на известный вам сайт, например, корпоративный портал. При переходе по ссылке, внутри сайт будет выглядеть абсолютно также, как оригинальный. Часто пользователь не особо внимательно смотрит на адрес сайта, а видит только знакомую картинку, где и пытается ввести свой логин и пароль. Большинство пользователей используют на всех своих ресурсах не более 3-4 паролей, и чаще всего это модификации одного и того же пароля. Мошенники таким образом получают разные пароли и пытаются уже использовать в своих целях.

Третий вариант - это заставить вас запустить нечто, что прислали вам уже в письме. Такой вариант называется “Троянский конь”. Такое письмо содержит в себе вложение, которое может нанести вред вашему компьютеру. Антивирусные программы на вашем компьютере проверяют всё, что поступает к вам в письме, но архивы и запароленные документы проверить не всегда могут. Другой вариант - это использование офисных документов, таких как Microsoft Word. К сожалению, внутри этих документов возможно внедрение вирусов. При использовании таких документов в них могут содержаться макросы. Это полноценный язык программирования, за которым можно написать всё, что угодно. Поэтому наличие макросов в простом документе должно вас насторожить.

На самом деле самым популярным способом фишинга является тайпсквоттинг, который появился ещё раньше, чем само понятие фишинг. Это

означает подмену букв в адресе знакомого нам сайта. С недавнего времени в именах сайтов стала разрешено использовать кириллицу. В результате мошенники латиницу в адресе подменяют на кириллицу, потому что написание некоторых букв в этих языках очень похоже. Это известный способ создания фальшивых сайтов, который используется до сих пор и является наиболее популярным [3].

Рассмотрим понятие “Троянский конь” в другом контексте, как попытку обмануть доверие пользователя. А именно попытка обмануть вас так, чтобы эксплуатировать ваше доверие. Например, одна из популярных фишинговых атак - это ночной звонок или SMS- сообщение о том, что ваши родные попали в беду. На такие звонки или сообщения попадались большинство людей. Выделяют 3 вида троянского коня: универсальный, сезонный и уникальный.

Универсальный рассчитан на большую площадь и на большую аудиторию людей. Как правило, эти атаки не очень хорошо подготовлены, рассчитаны либо на невнимательных людей, либо на людей совсем незнакомых с какими-то принципами интернета.

Сезонный фишинг является наиболее интересным. Такой сезонный фишинг можно было наблюдать несколько месяцев назад в связи с распространением коронавирусной инфекции. В этот момент появилось огромное количество фальшивых сайтов, где можно было зарегистрироваться, чтобы получить выплаты на семью, но получить их можно было только на госуслугах. В итоге из-за своей невнимательности или элементарных незнаний некоторые пользователи оставили свои личные данные на фальшивых сайтах. Рост спам - рассылок в это время отметили специалисты в зоне безопасности практически во всём мире.

Уникальный фишинг - самая большая и самая сложная тема с точки зрения сложности для мошенников. Она представляет из себя точечную атаку на конкретную организацию, у этой атаки есть конкретная цель. В организацию направляется письмо электронное с высокой степенью пробива именно этого контингента. Примером может служить фотосъёмка, которая была на корпоративном мероприятии. Рассылка делается всем сотрудникам якобы от фотографа, который предлагает просмотреть фотографии на стороннем ресурсе. Многие сотрудники в итоге переходят по вредоносной ссылке на фальшивый сайт. Главное для мошенников - правильно эту ситуацию эксплуатировать. Важно использовать какой-то принцип именно этой маленькой группы людей. Это необходимо для максимального пробива сайта данной организации. Еще один из способов называется “Квид про Кво” - это использование данных какой-то важной личности, то есть когда преступник пытается подменить собой личность знакомого нам с вами человека. Например, подмена вышестоящего руководителя вашей организации, с которым вы почти никогда не встречались и не разговаривали. Вероятнее всего, вы выполните его указания в письме. Многие люди в такой ситуации теряются и не могут здраво рассуждать и попадают на удочку мошенников. Такое письмо может содержать вредоносную ссылку, по которой человек перейдет, не подозревая об опасности [4].

Претекстинг - это четкий сценарий обмана жертвы, который расписан по минутам и секундам. Главная цель этого сценария - вывести жертву на какие-то действия. Самым популярным примером является звонок от сотрудника банка, который, конечно же, не является этим сотрудником. Весь разговор такого сотрудника направлен на то, чтобы узнать ваши личные данные в онлайн банке или вывести ваши денежные средства на посторонний счёт. Вас специально подводят к нужной точке разговора, торопят, не дают отвлекаться на другое.

Еще один вид фишинга называется “дорожное яблоко”. Часто таким предметом является флэш-карта. Человек поднимает находку, приносит ее на работу и из любопытства вставляет ее в рабочий компьютер. Дальше сценариев развития событий несколько. Первый - это размещённая вредоносная программа уже на носителе. Второй вариант - там будут разные папки, которые привлекут внимание большинства, например, фотографии. Среди этих фотографий может быть и программа, закамуфлированная под обычные фото. Ну и третий вариант: на китайских сайтах продажи товаров продаются устройства, закамуфлированные под флэш-накопитель, а на самом деле являются конденсаторами большой ёмкости. И когда вы втыкаете это устройство в компьютер, то просто сгорает материнская плата со всеми последствиями.

Ну и в завершение “**обратная социальная инженерия**”. Это тот случай, когда не мошенник появляется в вашей жизни, а вы появляетесь в жизни мошенника и даже не понимаете, что изначально вы к нему пришли. Один из таких популярных способов - это подмена телефонов и почтовых адресов на сайте организации. Если мошенник взломал какую-то организацию, он подменяет там почту и телефон. Если это сайт крупной организации, которую мы знаем, естественно, мы доверяем всей информации на их сайте.

Это основные виды фишинга. Понятно, что это разделение крайне условное, но в целом, наверное, покрывает 90% всего того, что бывает. Вы теперь готовы встретиться лицом к лицу с фишингом.

ОБСУЖДЕНИЕ

В ходе исследования были проанализированы особенности фишинговых атак, их разновидности.

Следует отметить, что сотрудники государственных организаций никогда не будут у вас спрашивать по телефону пароли и коды от личных электронных кабинетов, номера счетов. Нужно перезвонить лично и прояснить ситуацию.

Внимательное чтение электронных писем позволит избежать переходов на фальшивые сайты.

Проведение инструктажей по информационной безопасности сотрудников сможет обезопасить медицинские организации от фишинговых атак.

Спокойное и критичное отношение к звонкам с незнакомых номеров телефонов поможет сохранить сотрудникам финансы на своих банковских счетах.

Размещение на информационных стендах QR-кодов, адреса сайта медицинской организации с поясняющим текстом позволит пациентам избежать перехода на неверный адрес организации.

ВЫВОДЫ

1. Фишинговая стратегия имеет опасность с точки зрения защиты личных данных пациентов и медицинских учреждений.
2. Для пользователей во избежание фишинговых атак необходимо предпринимать следующие шаги:
 1. Программное обеспечение, установленное на ваших домашних и рабочих компьютерах, необходимо обновлять.
 2. Не нужно переходить по ссылкам из электронных писем, саму ссылку необходимо проверить в адресной строке.
 3. Не нужно открывать документы, полученные по почте, которые содержат макросы.

СПИСОК ИСТОЧНИКОВ

1. Что такое «фишинг»/ Энциклопедия Касперского// [Электронный ресурс]: <https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/> (дата обращения: 05.04.2022)
2. Кызыханов А.А., Байрушин Ф.Т. Фишинг как проблема для специалистов отдела ИБ/ [Электронный ресурс]: <https://cyberleninka.ru/article/n/fishing-kak-problema-dlya-spetsialistov-otdela-ib/viewer> (дата обращения: 05.04.2022)
3. Прокопайло А.А. Анализ фишинговых атак / [Электронный ресурс]: <https://cyberleninka.ru> (дата обращения: 05.04.2022)
4. 11 типов фишинга и их примеры из реальной жизни./ [Электронный ресурс]: https://club.cnews.ru/blogs/entry/11_tipov_fishinga_i_ih_primery_iz_realnoj_zhizni (дата обращения: 05.04.2022)

Сведения об авторах

А.В. Кузнецова – студент

С.И. Богданов – доцент, доктор медицинских наук

Information about the authors

A.V. Kuznetsova – student

S.I. Bogdanov – Doctor of Medicine, Associate professor

УДК 37.01:007

РАЗРАБОТКА ИНТЕРАКТИВНОГО ТРЕНАЖЕРА ДЛЯ ОТРАБОТКИ АЛГОРИТМА ДЕЙСТВИЯ ВРАЧА ПРИ ОФОРМЛЕНИИ РЕЦЕПТОВ У СТУДЕНТОВ МЕДИЦИНСКОГО ВУЗА

Лыкова Екатерина Александровна¹, Шадрин Софья Олеговна², Шестакова Анастасия Александровна³

¹⁻³ ФГБОУ ВО «Уральский государственный медицинский университет» Минздрава России, Екатеринбург, Российская федерация