МОШЕННИЧЕСТВО И ФИШИНГ В СЕТИ

ONLINE FRAUD AND PHISHING

УДК 004

Судаков Артём Владимирович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва, E-mail: artyom.sudakov.97@mail.ru

Грамзин Андрей Владимирович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Дудин Денис Артурович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Щербатюк Дарья Сергеевна, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Поремский Александр Романович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Sudakov Artyom Vladimirovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman Russia, Moscow

Gramzin Andrey Vladimirovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman Russia, Moscow

Dudin Denis Arturovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman, Russia, Moscow

Shcherbatyuk Daria Sergeevna, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman
Russia, Moscow

Poremsky Alexander Romanovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman
Russia, Moscow

Аннотация

В данной статье рассматриваются некоторые из современных видов мошенничества в сети Интернет, такие как фишинг и мошенничество с приобретением услуг и товаров в сети Интернет, а также простейшие способы защиты от них.

Ключевые слова: мошенники, аферисты, интернет, информация, кража, жертва, сведения, деньги, попасться, пароли, пин-коды.

Annotation

this article discusses some of the modern types of fraud on the Internet, such as phishing and fraud with the purchase of services and goods on the Internet, as well as the simplest ways to protect against them.

Ключевые слова: мошенники, аферисты, интернет, информация, кража, жертва, сведения, деньги, попасться, пароли, пин-коды.

Keywords: scammers, scammers, Internet, information, theft, victim, information, money, get caught, passwords, pin codes.

Появление сети - интернета началась с исследования компьютеров в 1950-х годах и возникновения научных и прикладных концепций массовых

вычислительных сетей в одно и то же время в государствах, а, в главную очередность в научных и военных лабораториях в США, Англии и Франции.

Сеть интернет-паутины — это массовая линия пользовательских компьютеров, который работает таким способом как почтовая структура, только со скоростью меньше секунды.

Там люди коротают время, учатся, честно работают, читают, играют и т. п.

Люди подписываются и получают полезные рассылки, покупают онлайн товары, билеты на самолет, поезд.

На некоторых мессенджерах проводятся многообразные возможные розыгрыши. Лотереи делаются большими торговыми площадками, престижных фирм, иногда — популярными пабликами в соцсетях или начинающими сеть интернет-маркетов.

Правдивых онлайн — лотерей мало, такие розыгрыши непременно жестко регламентируются. Участникам дают познакомиться с правилами на 10 листах, где указывается дословно каждый элемент розыгрыша.

Мир интернет-сети — увлекателен, комфортабелен и обширен кругозором. Несмотря на достоинства, присутствует одно - "НО" - Ни в коем случае нельзя забывать о мошенниках!

Цель данной работы – рассмотреть возможные способы мошенничества в сети интернета. Выявить способы, благодаря которым можно избежать махинаций злоумышленников.

Постановка проблемы:

Интернет-мошенничество — вид мошенничества с использованием интернета. Которое включает в себя сокрытие информации или предоставление неверной информации для вымогательства у жертв денег, имущества и наследства. Такое противозаконное занятие преследуется законодательством вне зависимости места совершения - в виртуальном или не виртуальном мире [1][2].

Задача аферистов — пригрести к рукам персональные сведения: выяснить ФИО, номер телефонного аппарата, пароли с учетных записей, паспортные сведения, реквизиты банковских карт и другую информацию.

Мошенники применяют такой способ для собственного допуска к чужим аккаунтам и переписке, а кроме того, в целях кражи финансов.

Для многочисленных крупных компании и сервисов, чтобы правильно функционировала работа, нужны личные сведения пользователей

При оформлении заказа в сети интернет нужна информация ФИО, местоположение и номер телефонного аппарата; при подписке в рассылку — электронная почта.

«Приобретение товаров и услуг посредством сети Интернет»

Покупать на интернет-ресурсах удобно. Особенно когда нет времени на живые походы по магазинам.

Мошенники обычно создают сайт или паблик и выкладывают товары одинакового визуального содержания. Цены стараются делать привлекательными.

Предоплата 100%

И после совершения такой оплаты вы не увидите ни заказ, ни денег [3].

Как не попасться?

Отсутствуют отклики, минимален интерфейс, показаны скромные контактные сведения. Больше всего подобные интернет-магазинчики функционируют согласно 100% предоплате. Переписка о приобретении товаров проводится с применением электронных почтовых ящиков и популярных мессенджеров. А также в последнее время очень распространенным видом такого мошенничества стал обман при помощи поддельных сайтов популярных интернет-сервисов для размещения объявлений. И чтобы не попасться на такие сайты необходимо всегда проверять адрес страницы, на которую вы переходите.

«Фишинг»

Мошенники вымогают у жертв пароли, пин-коды, номера и CVV-коды. Способов, которыми они могут получить нужные сведения большое количество:

Спам-рассылки от лжи - имени легальных органов, в которых указания войти в "сеть интернет-сайт-двойник" подобного учреждения и подтвердить пароли, пин-коды и другую информацию, используют в последующем злоумышленники с целью кражи денег со счета жертвы. Распространенным представляет собой предложение работы за границей, уведомление о выигрыше в лотереи, а помимо этого информации о получении наследства [4].

Как не попасться?

Заранее предвидеть действия аферистов не легко, однако в случае если никак не дозволять себе увлечься и хладнокровно подходить к каждому сомнительному оповещению с осторожностью: проверять многократно, то появится шанс не быть жертвой фишинга.

В массе случаев аферисты не стремятся утаить местоположение, откуда поступают небезопасные уведомления и небрежно выдают себя за доверенного поставщика услуг.

У мошенников отсутствует местоположение с домена банка.

Взамен этого можно отыскать домен *.com.ru либо *.org.ru вместо *.ru, который применяется экономическими учреждениями, действующими на территории России.

Аферисты иногда хитроумны и применяют адреса, похожие на службы, которые воплощают, но различаются от оригинала не большими деталями, подобными как содержание послания или инструкции к ним.

Уделяйте чуткое внимание в уведомлениях электронной почты - адресам страничек, на которые отправители ссылаются.

Вопреки наружному виду не нужно нажимать на них, чтобы заметить, куда перенесет электронный адрес. Попросту наведите курсор мыши на ссылку и подождите, до тех пор, пока интернет-браузер или программа электронной

почты не продемонстрирует URL, который прячется под текстом. Главное внимание следует отдавать сайтам, которые не относятся к предложенным уведомлениям.

Выводы:

Виды мошенничества в сети не ограничиваются только такими способами обмана. В данной статье разобраны самые распространённые и популярные обманы среди аферистов. Их неимоверное количество и злоумышленники с каждым разом придумывают новые способы, чтобы обокрасть честных людей.

Аферисты сидят не только в сети интернет. Поэтому нужно быть бдительными и внимательными и в реальном мире.

Сейчас существует множество защитных программ для ПК и мобильных устройств: антиспам, определитель спама, индикация и защита личных страниц на мессенджерах, антивирусы и другие.

Будьте бдительны, и пусть вам никогда не встречаются такие не хорошие люди на жизненном пути.

Литература

1. Интернет-мошенничества – уголовная ответственность: [Электронный ресурс]. URL: https://07.xn--b1aew.xn--p1ai/news/item/11911464 (дата обращения: 20.05.2021)
2. Интернет-мошенничество - памятка для граждан: [Электронный ресурс]. URL: https://мвд.рф/document/1910260 (дата обращения: 20.05.2021)
3. Обман в Интернете: как не стать жертвой мошенников | Hi-Tech |Селдон Новости: [Электронный ресурс]. URL: https://news.myseldon.com/ru/news/index/235795585 (дата обращения: 20.05.2021)
4. Как распознать фишинг и как ему противостоять, все о фишинге: [Электронный ресурс]. URL: https://root-nation.com/ru/posts/internet-posts/ru-phishing-kak-emu-protivostoyat (дата обращения: 20.05.2021)

Literature

1. Internet fraud - criminal liability: [Electronic resource]. URL: https: //07.xn--b1aew.xn--p1ai/news/item/11911464 (date accessed: 20.05.2021)
2. Internet fraud - a memo for citizens: [Electronic resource]. URL: https: //mv.d.rf/document/1910260 (date accessed: 20.05.2021)
3. Cheating on the Internet: how to avoid becoming a victim of scammers | Hi-Tech | Seldon News: [Electronic resource]. URL: https://news.myseldon.com/ru/news/index/235795585 (date accessed: 20.05.2021)
4. How to recognize phishing and how to resist it, everything about phishing: [Electronic resource]. URL: https://root-nation.com/ru/posts/internet-posts/ru-phishing-kak-emu-protivostoyat (date accessed: 20.05.2021)