Научная статья
Original article
УДК 004.424

ФИШИНГ И ВИШИНГ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

PHISHING AND VSHING IN INFORMATION SECURITY

Куренная Валерия Олеговна, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kurennaya Valeria Olegovna, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. В данной статье описан вишинг, как один из методов как пользователей. Вишинг представляет собой голосовой фишинг, и направлен на киберпреступление, при котором злоумышленники используют телефон для кражи личной информации своих целей. При вишинг-атаке киберпреступники используют тактику социальной инженерии, чтобы убедить жертв предоставить личную информацию, как правило, с целью доступа к финансовым счетам.

Annotation. This article describes vishing as one of the methods as users. Vishing is voice phishing and is a cybercrime in which attackers use a phone to steal the personal information of their targets. In a vishing attack, cybercriminals use social engineering tactics to convince victims to provide personal information, usually in order to access financial accounts.

Ключевые слова: фишинг, вишинг, информационная безопасность.

Key words: phishing, vishing, information security.

Целевые фишинговые угрозы-это повышенная форма фишинговых вирусных атак, которые используют социальную инженерию, чтобы заставить конкретного человека раскрыть конфиденциальную информацию. Целенаправленные фишинговые атаки достигают успеха, используя информацию, почерпнутую из социальных сетей и других источников, чтобы создать ощущение знакомства. Так, например, электронные письма, которые были присланы «жертве», могут упоминать общего друга, ссылаться на недавнюю покупку или включать информацию, которая, по-видимому, является надежным источником.

После того, как было установлено доверие, целевые фишинговые кампании просят получателя предоставить некоторую информацию или войти на веб-сайт, который оказывается фальшивым или зараженным вредоносными программами.

Чтобы предотвратить фишинговые атаки и целевые фишинговые атаки, организациям нужны мощные инструменты для выявления подозрительной электронной почты и предотвращения действий сотрудников по ним.

Атака может развиваться следующим образом:

Преступник исследует имена сотрудников в отделе маркетинга организации и получает доступ к последним счетам.

Выступая в роли директора по маркетингу, злоумышленник отправляет электронное письмо менеджеру проекта отдела, используя строку темы, которая гласит: Обновленный счет для кампаний Q3. Текст, стиль и прилагаемый логотип дублируют стандартный шаблон электронной почты организации.

Что такое вишинг-атака?

Вишинг, также известный как голосовой фишинг, представляет собой киберпреступление, при котором злоумышленники используют телефон для кражи личной информации своих целей. При вишинг-атаке киберпреступники

используют тактику социальной инженерии, чтобы убедить жертв предоставить личную информацию, как правило, с целью доступа к финансовым счетам.

Как и при традиционном фишинге (на основе сообщений электронной почты) или смишинге (на основе текстовых сообщений), при вишинге злоумышленник должен убедить жертву в том, что он поступает правильно, сотрудничая с киберпреступником. Злоумышленник может притвориться, что представляет полицию, правительство, налоговый департамент, банк или работодателя жертвы.

Киберпреступники используют убедительный язык и угрозы, чтобы заставить жертву поверить, что у нее нет другого выбора, кроме как передать запрошенные данные. Некоторые киберпреступники используют агрессивные выражения, другие предлагают помочь жертве избежать уголовного преследования, а третьи притворяются ИТ-специалистами, занимающимися обслуживанием устройства пользователя. Еще одна тактика, которую используют киберпреступники, оставляя голосовые сообщения, сообщая жертве, что, если она не перезвонит, она рискует получить серьезные последствия.

Самый эффективный способ предотвратить вишинг — инвестировать в осведомленность о безопасности, обучая сотрудников распознавать схемы вишинга и избегать сотрудничества с злоумышленниками.

Вишинг против фишинга: в чем разница?

Вишинг и фишинг имеют одну и ту же цель: получить конфиденциальную информацию от пользователей, которую киберпреступники могут использовать для получения денег, кражи личных данных или захвата учетной записи. Основное различие между вишинговыми и фишинговыми атаками заключается в методах, которые злоумышленники используют для нацеливания на жертв: фишинг — это в основном атака на основе электронной почты, тогда как вишинг использует телефонную линию.

Обычно и фишеры, и вишеры бомбардируют свои цели большими объемами сообщений. Фишинговый злоумышленник может отправить большое количество электронных писем по списку возможных целей. Злоумышленники, решившие атаковать определенную организацию, могут атаковать адреса электронной почты, принадлежащие пользователям с высоким уровнем привилегий из этой организации.

Фишеры, как правило, используют убедительные сообщения, чтобы убедить пользователей ответить конфиденциальными данными или убедить их щелкнуть ссылку, связанную с вредоносным ПО. Некоторые фишинговые злоумышленники будут использовать вредоносные вложения.

Вишер мог сначала отправить большой объем текстовых сообщений возможным жертвам из списка телефонных номеров. Сообщение может побудить жертву позвонить на телефон киберпреступника. В качестве альтернативы злоумышленники Visher могут создать автоматическое сообщение, которое робо-звонит возможным жертвам. Этот метод основан на компьютерных голосовых сообщениях, удалении акцентов и установлении доверия.

Затем злоумышленник обманом заставляет жертв следовать инструкциям в голосовом сообщении, которое соединяет их с агентом-человеком. Агент может продолжить мошенничество или направить пользователей на создание веб-сайта, контролируемого злоумышленником.

Люди, которые знают о фишинге, могут не знать о вишинге, поэтому, используя эту новую технику, киберпреступники увеличивают свои шансы на успех.

Примеры вишинг-атак

Большинство случаев мошенничества связано с общением по телефону. Вот несколько примеров распространенных вишинг-атак:

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного

интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.

2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Куренная В.О., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Куренная В.О. ФИШИНГ И ВИШИНГ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.