УДК 004.056.53

ФИШИНГ КАК ПРОБЛЕМА СОВРЕМЕННОГО ОБЩЕСТВА

Долгая А.С., Майорова Е.А.
гр. 361402
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Научный руководитель: Пухир Г.А. — старший преподаватель кафедры защиты информации

Аннотация. В материалах статьи рассматривается такой вид интернет-мошенничества как фишинг, его типы, основные методы борьбы с ними. Защита от фишинга в приоритете ставит информированность пользователей о таком виде атаки с целью исключения человеческого фактора.

Ключевые слова: фишинг, программное обеспечение, защита информации

Введение. В современном мире стремительно происходит процесс цифровизации. Как результат, все сферы жизни подверглись изменениям. Даже преступления теперь совершаются посредством сети Интернет. Одним из самых распространённых примеров можно назвать фишинг. Фишинг (phishing) (выуживание идентификаторов) – способ получения идентификаторов пользователя информационных систем нарушителем, который основан на предоставлении пользователю такой информации и создании нарушителем таких

условий ее восприятия, при которых пользователь примет ошибочное решение и в результате чего выполнит некоторое действие, которое является выгодным нарушителю.

Основная часть. Проблема фишинга крайне актуальна среди обычных пользователей, активно использующих информационные технологии в бытовой сфере. К примеру, в 2023 году почти половина (43%) всех успешных атак на организации были проведены с использованием социальной инженерии[1] (79% из них осуществлялись через электронную почту, СМС-сообщения, социальные сети и мессенджеры).

Существуют следующие виды фишинга:

- Почтовый — сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат, вложения в виде файла или гипертекстовой ссылки на файл, загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя;
- Онлайновый — сообщения, которые формирует нарушитель, передаются посредством электронной почты. Такие сообщения кроме текста содержат, вложения в виде файла или гипертекстовой ссылки на файл, загрузка которого или переход по которой приводит к загрузке и установке вредоносной программы на устройство пользователя;
- Целенаправленный — (спиарфишинг, spear - гарпун) - сообщения, которые формирует нарушитель, передаются посредством электронной почты. Их текст адресован конкретному человеку, так как нарушитель до составления такого сообщения смог получить доступ к персональным данным этого человека;
- Вишинг — реализуется с помощью средств IP (IP –internet protocol) телефонии (мессенджеры) – это позволяет скрыть адрес нарушителя и управлять действиями человека с помощью речи.

Целенаправленный фишинг является самым опасным, так как полученные заранее данные о жертве вызывают у нее доверие. Чтобы противостоять фишингу важно знать как он работает. Цепочка событий при реализации фишинговой атаки может быть рассмотрена на примере широко известной модели атаки Cyber-Kill Chain [статья «The Industrial Control System Cyber-Kill Chain» авторства Майкла Дж. Ассанта и Роберта М. Ли]. Сценарий, по которому работает злоумышленник, включает в себя сбор информации об атакуемом объекте, внедрение в систему (например, загрузка и установка вредоносного программного обеспечения) и активация вредоносных действий.

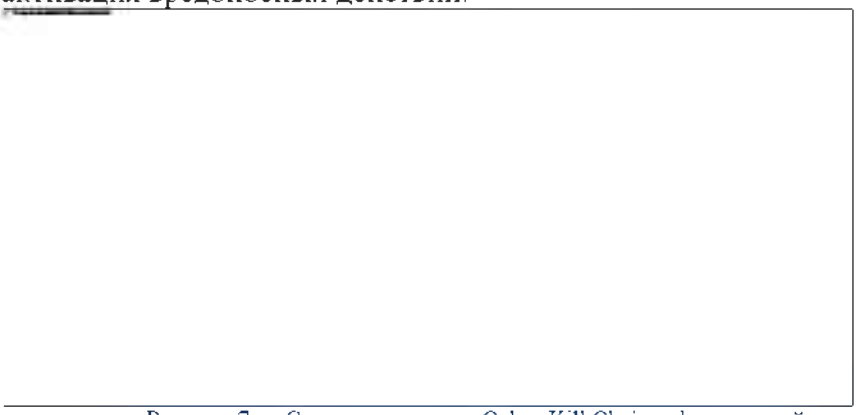

Рисунок 7 — Сравнение модели Cyber-Kill Chain и фишинговой

На рисунке 1 мы можем видеть сравнение модели атаки Cyber-Kill Chain и фишинговой атаки. Они происходят по сходному принципу. Как и Cyber-Kill Chain, фишинговая цепочка начинается с подготовки нарушителя (сбор контактов, подготовка инфраструктур), затем нарушитель воздействует на эмоциональное состояние жертвы и

[1] **Социальная инженерия** - метод управления действиями пользователя информационной системы, основанный на введении его в эмоциональное состояние таким образом, чтобы нейтрализовать его критическое мышление на то время, когда он будет совершать выгодное действие под управлением нарушителя

предпринимает некоторые действия для получения его идентификаторов (обман, клик, ввод данных). Успешная реализация этих пунктов неизбежно приводит к реализации атаки (кража данных, действие).

Для защиты от подобного рода атак существуют разные подходы, позволяющие разорвать цепочку событий, запущенных злоумышленником. При этом, чем раньше будет обнаружена угроза, тем эффективнее можно противостоять фишингу. Чтобы не стать жертвой фишинга, зачастую, достаточно сохранять критическое мышление и уметь распознавать подозрительные сообщения и ссылки. Это как раз и позволит на первых этапах остановить развитие опасных для конфиденциальной информации пользователя событий.

Другой подход использует автоматизированные системы, анализирующие содержимое файлов, почтовых писем и другого контента, который может содержать вредоносный код или ссылку на него. Также существуют программное обеспечение, предназначенное для защиты от фишинга. Среди прочих, можно выделить отдельные примеры таких программ [https://1csoft.ru/catalog/programmy-dlya-zashchity-ot-fishinga]:

- Dallas Lock — сертифицированная система защиты конфиденциальной и секретной (до уровня совершенно секретно включительно) информации от несанкционированного доступа накладного типа в персональных компьютерах с ОС семейства Windows. Обеспечивает: защиту от руткитов, защиту от фишинга, защиту USB-устройств, DLP-системы, защиту от утечки данных, межсетевой экран.
- NANO Антивирус Pro — надежный и удобный продукт от российского разработчика, предназначенный для защиты персонального компьютера под управлением операционной системы Windows от всех типов вредоносных программ – шифровальщиков, блокировщиков экрана, банковских троянских программ, потенциально нежелательных программ, рекламных программ, программ-шпионов и т.д. Специализируется именно на защите от фишинга.
- PRO32 Ultimate Security — комплексное решение премиум-класса для информационной безопасности. Обеспечивает защиту устройств Windows и Android от современных киберугроз и вредоносных программ, включает функции резервного копирования и восстановления для предотвращения потери данных.
- Антивирус Касперского для файловых серверов — эффективно защищает файловые серверы, работающие под управлением Microsoft Windows, Linux и Novell NetWare, от всех видов вредоносных программ. Антивирусная защита сетевых хранилищ общего доступа очень важна, поскольку один-единственный зараженный файл на сервере может стать источником заражения всех компьютеров вашей корпоративной сети. Современные требования к решениям для защиты файловых серверов включают стабильность работы продукта и эффективное использование системных ресурсов.

Заключение. Как мы видим, в современном обществе созданы благоприятные условия для защиты от фишинга. Технологии кибератак совершенствуются, как и методы борьбы с ними. Тогда как психология человека заложена природой, поэтому главной проблемой остается лишь неосведомленность людей о методах противодействиях ему. Нарушители постоянно создают новые способы обмана, поэтому необходимо регулярно повышать уровень информированности людей.

Список литературы:

1. *1Soft. Программы для защиты от фишинга [Электронный ресурс]. — Режим доступа : https://1csoft.ru/catalog/programmy-dlya-zashchity-ot-fishinga. — Дата доступа : 28.02.2024.*
2. *Международный журнал прикладных и фундаментальных исследований. Анализ проблемы фишинга в цифровом пространстве [Электронный ресурс]. — Режим доступа : https://applied-research.ru/ru/article/view?id=13594. Дата доступа: 28.02.2024*
3. *Positive technologies. Тренды фишинговых атак на организации в 2022-2023 годах [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/phishing-attacks-on-organizations-in-2022-2023/#id10. Дата доступа : 29.02.2024*
4. *M. J. Assante. R. M. Lee. The Industrial Control System Cyber Kill Chain / M. J. Assante, R. M. Lee. — SANS Institute, 2015. — 2 с.*

UDC 004.056.53

PHISHING AS A PROBLEM OF MODERN SOCIETY

Dolgaya A.S., Mayorova Y.A.
gr. 361402

Belarusian State University of Informatics and Radioelectronics,
Minsk, Republic of Belarus

Puhir H.A. — Senior Lecturer of the Department of Information Protection

Annotation. In the materials of the article is considered this kind of Internet fraud as phishing, its types, the main methods of dealing with them. Protection against phishing prioritizes users' awareness of this type of attack to eliminate the human factor.

Keywords: phishing, software, information protection