БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 2 (113). – 69–78

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-2-69-78

УГРОЗА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ФИШИНГА В СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

Н.Е. КАРПОВА[1], И.И. ВОСКАНЯН[2]

[1] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: esib@samgtu.ru*
[2] *443071, РФ, г. Самара, ул. Конноармейская, 17, инженер ООО «Газинформсервис». E-mail: naynaksov@gmail.com*

Информация – важнейший ресурс любой компании в наше время, поэтому обеспечение ее защиты является одной из приоритетных бизнес-задач каждой организации.
С течением времени технические системы защиты всё больше и больше совершенствуются за счет развития технологий, учета множества каналов утечек информации и увеличения потребности в обеспечении информационной безопасности в целом. Грамотно выстроенные технические системы защиты всегда будут выполнять возложенные на них задачи, но один-единственный фактор может сделать их бесполезными – это человек. Люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами и ошибками, являясь самым слабым звеном в цепочке безопасности.
Поэтому начали набирать популярность атаки, направленные не на саму систему, а на ее пользователей, так называемые социоинженерные атаки.
В настоящей статье рассмотрены вопросы угроз социальной инженерии и фишинга в современной информационной безопасности. Во время выполнения работы были проанализированы история и принцип работы социальной инженерии.
В результате работы был представлен пример настоящей фишинговой атаки (пентеста), произведен анализ статистических данных. Были представлены выводы об угрозе фишинга.

Ключевые слова: информационная безопасность, каналы утечки информации, пользователь, социальная инженерия, фишинг, угрозы, пентест, аттракция, система защиты

* Статья получена 29 апреля 2024 г.

ВВЕДЕНИЕ

Сейчас информация стала неотъемлемым и основополагающим ресурсом для любой компании. В связи с этим обеспечение безопасности информации стало одним из ключевых приоритетов всех организаций.

Качественные технические системы безопасности всегда будут выполнять свои задачи, однако их эффективность может быть подорвана одним фактором – человеком.

Поэтому эксплуатация «человеческого фактора» становится всё более популярной, так как позволяет обойти системы безопасности и сделать их бесполезными, попросту игрушками. Такой вид воздействия получил название «социальная инженерия».

Впервые в научном обороте понятие «социальная инженерия» было применено в СССР Алексеем Капитоновичем Гастевым – руководителем Центрального института труда (г. Москва), однако он рассматривал это понятие как науку, которая позволяет достичь максимальной производительности сотрудника на рабочем месте путем управления его психологическим состоянием.

Современная социальная инженерия эволюционировала в совокупность подходов прикладных социальных наук, ориентированных на целенаправленное изменение организационных структур, определяющих человеческое поведение [7].

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Обобщенный алгоритм атаки социального инженера в наши дни приведен на рис. 1.

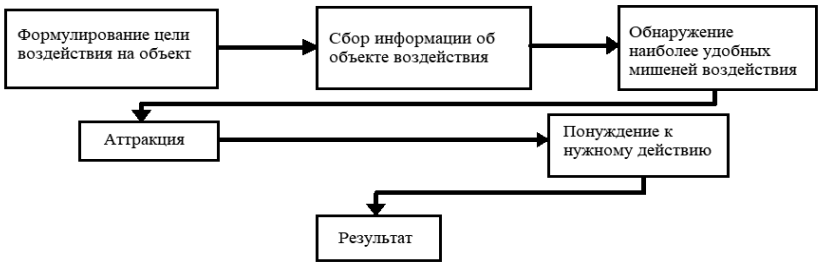

Рис. 1. Обобщенный алгоритм атаки социального инженера

Важнейшим аспектом атаки является аттракция (от лат. attrahere – привлекать, притягивать) – создание нужных условий для воздействия социоин-

женера на цель. Это включает в себя принуждение к желаемым действиям, когда объект воспринимает их как собственные и впоследствии принимает решение выполнить необходимые социоинженеру действия, думая, что они происходят по его собственной воле. То есть аттракция – это вхождение в доверие к жертве [4].

Существует множество разновидностей социальной инженерии – от так называемого «дорожного яблока» до «претекстинга», но, основываясь на статистике, которая приведена на рис. 2, наиболее распространенныи и опасными считаются фишинговые атаки.

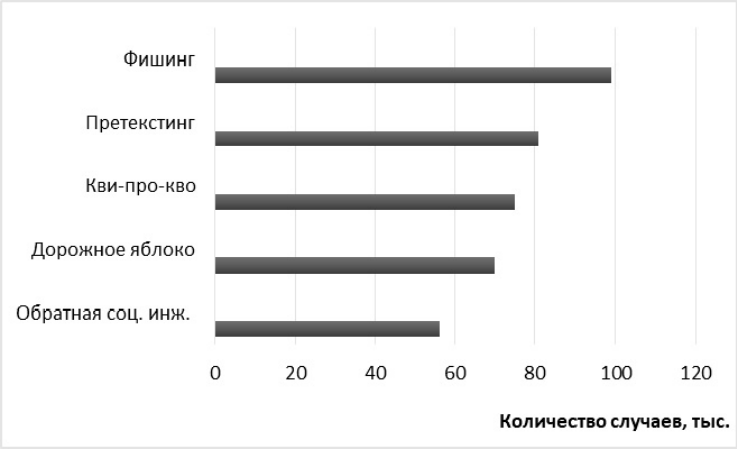

Рис. 2. Статистика атак социальной инженерии за 2021 год

Фишинг – это тип киберпреступления, при котором преступники выдают себя за надежный источник в Интернете, чтобы вынудить жертву передать им личную информацию (например, имя пользователя, пароль, номер банковской карты и пр.) [8].

В отличие от других интернет-угроз, фишинг не требует обладания высоким уровнем технического знания.

Фишинговые мошенники не пытаются использовать технические уязвимости в операционной системе устройства, вместо этого они прибегают к методам социальной инженерии. Нет ни одной операционной системы, которая бы обладала полной защитой от фишинга, несмотря на силу ее антивирусных средств. Фактически злоумышленники часто выбирают фишинг как метод, потому что не могут найти технические уязвимости. Зачем тратить время на взлом сложной системы защиты, когда можно обмануть пользователя и заста-

вить его добровольно раскрыть свои данные? В большинстве случаев самым уязвимым моментом в защите системы является не ошибка, затаенная глубоко в программном коде, а сам пользователь, который не обращает внимания на отправителя очередного электронного письма.

Фишинг имеет огромное разнообразие подходов, но общим аспектом всех атак является применение обмана с целью выманивания ценностей или информации.

Говоря о фишинге и о методах защиты от него, нельзя не упомянуть тестирование на проникновение (пентест). Это метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Анализ ведется с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Цель испытаний на проникновение — оценить возможность его осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. Результатом проведения испытания на проникновение, как правило, является отчет, содержащий выявленные в ходе анализа уязвимости и опционально рекомендации по их устранению [9].

ИССЛЕДОВАНИЕ

Рассмотрим типичную фишинговую атаку (пентест) на примере личного кабинета СамГТУ https://lk.samgtu.ru/:

Настоящая страница личного кабинета приведена на рис. 3.

Рис. 3. Настоящая страница личного кабинета

На рис. 4 приведена фишнговая страница.

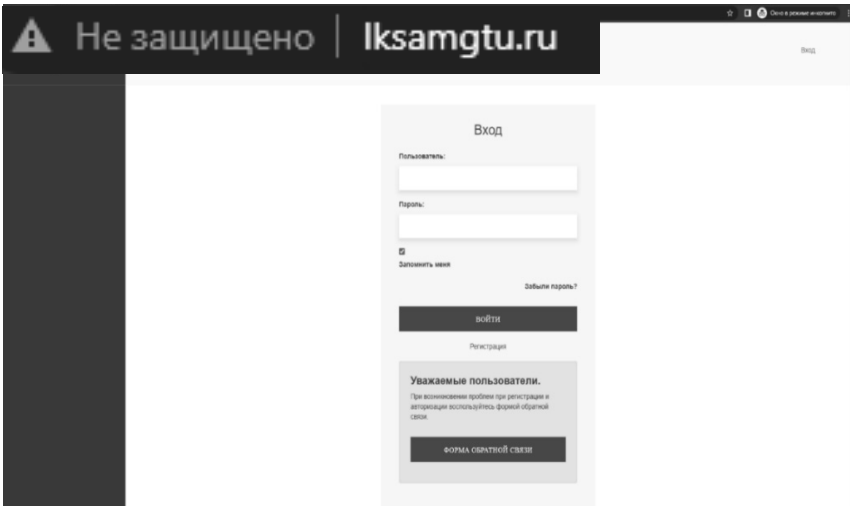

Рис. 4. Фишинговая страница личного кабинета

Письмо, содержащее аттракцию, представлено на рис. 5.

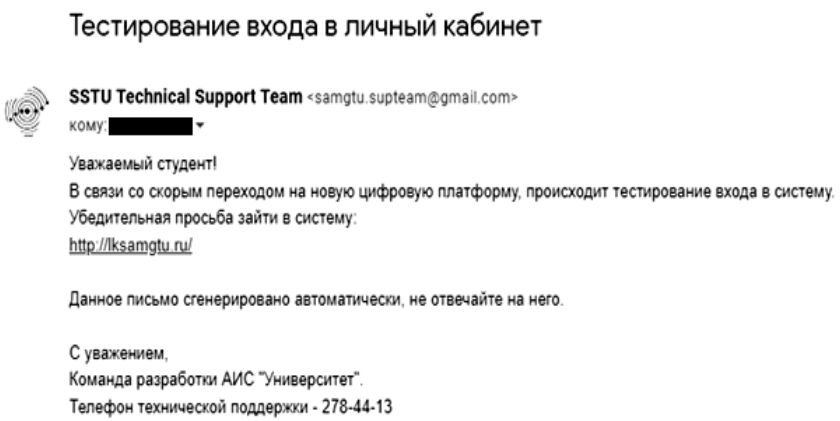

Рис. 5. Фишинговое электронное письмо

Такая, казалось бы, простейшая и банальная атака на студентов одного из крупнейших технических вузов страны выявила статистику, представленную на рис. 6.

Рис. 6. Статистика фишинговой атаки

Более половины испытуемых оказались уязвимы к фишинговой атаке и являются потенциальными жертвами социального инженера.

На основе фишинговых атак могут начинаться более сложные кибератаки, такие как заражение компьютеров, перехват управления технологическими процессами или нарушение работы системы. Поэтому сотрудники четко должны знать, как противостоять фишингу.

Основополагающим элементом для защиты от атак социальной инженерии являются пользователи с высоким уровнем знаний в области информационной безопасности, именно с ними нужно работать, чтобы обезопасить свою организацию.

Регулярные тестирования на проникновение с помощью тестовых фишинговых атак являются отличным методом для повышения уровня компетентности в области информационной безопасности сотрудников организации.

ЗАКЛЮЧЕНИЕ

Социальная инженерия как наука зародилась именно в нашей стране. Но ее функция отличалась от современной социальной инженерии. А.К. Гастев разработал и изучал эту науку, чтобы понять, как добиться максимальных результатов от сотрудников на их рабочем месте.

Социальная инженерия приобрела свой современный облик в 1980-х годах. С тех пор проблема подобных атак становится всё более серьезной. Появляются новые и изощренные методы и стратегии обмана самой сильной, но в то же время самой уязвимой системы – человека.

Самым распространенным методом атак социальной инженерии является фишинг. Каждый человек сталкивается с подозрительными электронными письмами, СМС-сообщениями или звонками. Ежегодно миллионы людей и тысячи организаций становятся жертвами фишинговых атак, что влечет за собой потерю миллионов долларов.

Угроза взлома, который нарушит секретность вашей жизни или информационной системы вашей компании, может казаться не настолько реальной, пока это не произойдет однажды. Чтобы избежать столь дорогостоящей дозы действительности, нам нужно стать осведомленными, образованными, бдительными и настойчиво защищать наши информационные активы, нашу собственную персональную информацию и наши национальные критичные инфраструктуры. И мы должны научиться этому уже сегодня.

СПИСОК ЛИТЕРАТУРЫ

1. *Гастев А.К.* Как надо работать: практическое введение в науку организации труда. – Изд. 2-е. – М.: Экономика,1972. – 478 с.

2. *Гастев А.К.* Социальные установки // У истоков НОТ: забытые дискуссии и нереализованные идеи. – Л., 1990. – С. 103.

3. *Гастев А.К.* Трудовые установки. – М.: Экономика, 1973. – 343 с.

4. *Генне О.В.* Заметки о социальной инженерии // Защита информации. Инсайд. – 2006. – № 6 (12). – С. 16–19.

5. *Митник К., Саймон У.* Искусство обмана. – М.: АйТи, 2004. – ISBN 5-98453-011-2. – ISBN 0-471-23712-4.

6. *Sammons J.* The basics of digital forensics: the primer for getting started in digital forensics. – Elsevier Science, 2012. – 177 p. – ISBN 9781597496612.

7. Инженерия социальная // Российская социологическая энциклопедия / под общ. ред. Г.В. Осипова. – М.: Норма–Инфра-М, 1999. – URL: https://sociologicheskaya.academic.ru/392 (дата обращения: 31.05.2024).

8. Все о фишинге. – URL: https://ru.malwarebytes.com/phishing/ (дата обращения: 31.05.2024).

9. *Музалевский Ф.А.* Что такое пентест? – URL: https://rtmtech.ru/articles/chto-takoe-pentest/ (дата обращения: 31.05.2024).

10. *Романов В.Г., Романова И.В.* Социальное мошенничество «COVID-19» и манипулятивные технологии социальной инженерии // Вестник Забайкальского государственного университета. – 2020. – Т. 26, № 9. – С. 57–67.

11. *Дьяков Н.В.* Применение методов социальной инженерии в социальных сетях // // Общество. – 2020. – № 2 (17). – С. 126–128.

12. *Румянцев Е.П., Найденов Н.Д.* Виды фишинга и способы защиты от него // Аллея науки. – 2018. – № 6 (22). – С. 451–455.

13. *Штайгер А.А.* Социальная инженерия на примере фишинга // Вестник современных исследований. – 2018. – № 6.3 (21). – С. 612–614.

14. 11 типов фишинга и примеры из реальной жизни. – URL: https://www.cloudav.ru/mediacenter/tips/types-of-phishing/ (дата обращения: 31.05.2024).

15. Как избежать атаки с использованием социальной инженерии / Лаборатория Касперского. – URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks (дата обращения: 31.05.2024).

Карпова Надежда Евгеньевна, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основные направления научных исследований – автоматизированные интеллектуальные системы и автоматизированные информационно-измерительные системы. Имеет более 100 публикаций. E-mail: esib@samgtu.ru

Восканян Игит Игитович, инженер ООО «Газинформсервис». E-mail: naynaksov@gmail.com

DOI: 10.17212/2782-2230-2024-2-69-78

Threat of social engineering and phishing in modern information security*

N.E. Karpova[1], I.I. Voskanyan[2]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate professor of the electronic systems and information security department. E-mail: esib@samgtu.ru*
[2] *«Gazinform», 17 Konneramiyskaya Street, Samara, 443071, Russian Federation, engineer of «Gazinform». E-mail: naynaksov@gmail.com*

Information is the most important resource of any company in our time, so ensuring its protection is one of the priority business tasks of each organization.
Over the years, technical security systems have been increasingly improved through technological developments, the recording of multiple channels of information leakage and the growing need for information security in general. Well-designed technical protection systems will always perform the tasks assigned to them, but one single factor can make them useless – a person. People will remain human, with their weaknesses, prejudices, stereotypes and mistakes, being the weakest link in the security chain.
So attacks started to gain popularity, targeting not the system itself, but its users, the so-called social engineering attacks.
In this article the issues of threats of social engineering and phishing in modern information security are considered. During the work the history and principle of social engineering were analyzed.
As a result, an example of a real phishing attack (penteste) was presented, the analysis of statistical data was made. Conclusions about the phishing threat were presented.

Keywords: Information security, Information leakage channels, User, Social engineering, Phishing, Threats, Pentest, Attraction, Security system

REFERENCES

1. Gastev A.K. *Kak nado rabotat': prakticheskoe vvedenie v nauku organizatsii truda* [How to work. Practical introduction to the science of the organization of labor]. 2nd ed. Moscow, Ekonomika Publ., 1972. 478 p.

2. Gastev A.K. Sotsial'nye ustanovki [Social Attitudes]. *U istokov NOT: zabytye diskussii i nerealizovannye idei* [Origins of NOTE: Forgotten discussions and unrealized ideas]. Leningrad., 1990, p. 103.

3. Gastev A.K. *Trudovye ustanovki* [Industrious routine]. Moscow, Ekonomika Publ., 1973. 343 p.

4. Genne O.V. Zametki o sotsial'noi inzhenerii [Notes on social engineering]. *Zashchita informatsii. Insaid*, 2006, no. 6 (12), pp. 16–19. (In Russian).

* *Received 29 April 2024.*

5. Mitnick K., Simon W. *Iskusstvo obmana* [Art of deception]. Moscow, AiTi Publ., 2004. ISBN 5-98453-011-2. ISBN 0-471-23712-4. (In Russian).

6. Sammons J. *The basics of digital forensics: the primer for getting started in digital forensics*. Elsevier Science, 2012. 177 p. ISBN 9781597496612.

7. Inzheneriya sotsial'naya [Engineering social]. *Rossiiskaya sotsiologicheskaya entsiklopediya* [Russian sociological encyclopedia]. Moscow, Norma–Infra-M Publ., 1999. Available at: https://sociologicheskaya.academic.ru/392 (accessed 31.05.2024).

8. *All about Phishing*. Available at: https://www.malwarebytes.com/phishing (accessed 31.05.2024).

9. Muzalevskii F.A. *Chto takoe pentest?* [What is pentest?]. Available at: https://rtmtech.ru/articles/chto-takoe-pentest/ (accessed 31.05.2024).

10. Romanov V.G., Romanova I.V. Sotsial'noe moshennichestvo «COVID-19» i manipulyativnye tekhnologii sotsial'noi inzhenerii [Social fraud-covid-19 and manipulative social engineering technologies]. *Vestnik Zabaikal'skogo gosudarstvennogo universiteta = Transbaikal State University Journal*, 2020, vol. 26, no. 9, pp. 57–67.

11. Dyakov N.V. Primenenie metodov sotsial'noi inzhenerii v sotsial'nykh setyakh [Application of social engineering methods in social networks]. *Obshchestvo = Society*, 2020, no. 2 (17), pp. 126–128.

12. Rumyantsev E.P., Naidenov N.D. Vidy fishinga i sposoby zashchity ot nego [Types of phishing and ways of protection against it]. *Alleya nauki = Alley of Science*, 2018, no. 6 (22), pp. 451–455.

13. Shtaiger A.A. Sotsial'naya inzheneriya na primere fishinga [Social engineering by example of phishing]. *Vestnik sovremennykh issledovanii*, 2018, no. 6.3 (21), pp. 612–614. (In Russian).

14. *11 tipov fishinga i primery iz real'noi zhizni* [11 types of phishing + real-life examples]. Available at: https:///www.cloudav.ru/mediacenter/tips/tips/types-of-phishing/ (accessed 31.05.2024).

15. Kaspersky Lab. *Kak izbezhat' ataki s ispol'zovaniem sotsial'noi inzhenerii* [How to avoid an attack using social engineering]. Available at: https://ww.kaspersky.ru/resource-center/threats/how--avoid-social-engeringattacks (accessed 31.05.2024).

Для цитирования:

Карпова Н.Е., Восканян И.И. Угроза социальной инженерии и фишинга в современной информационной безопасности // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 69–78. – DOI: 10.17212/2782-2230-2024-2-69-78.

For citation:

Karpova N.E., Voskanyan I.I. Ugroza sotsial'noi inzhenerii i fishinga v sovremennoi informatsionnoi bezopasnosti [Threat of social engineering and phishing in modern information security]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 2 (113), pp. 69–78. DOI: 10.17212/2782-2230-2024-2-69-78.