Перевертун Д.Р. Как защититься от социальной инженерии: стратегии и тактики // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 9(35) с. 50–53

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

# КАК ЗАЩИТИТЬСЯ ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: СТРАТЕГИИ И ТАКТИКИ

**Перевертун Д.Р.**
*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: danilaperevertun@gmail.com*

**В данной статье рассматривается одна из наиболее актуальных и опасных угроз в области информационной безопасности - социальная инженерия. Автор предоставляет стратегии и тактики, которые помогут как индивидам, так и организациям укрепить свою защиту от манипуляций и атак, направленных на человеческий фактор. Статья акцентирует внимание на важности обучения и осведомленности сотрудников, бережливости в обращении с конфиденциальной информацией, использовании двухфакторной аутентификации, подозрительности и постоянном обновлении методов защиты. Читатели получат практические советы и инструкции, которые помогут им лучше защитить свои личные и корпоративные данные от социальных инженеров.**

Ключевые слова: Социальная инженерия, информационная безопасность, манипуляция, обучение по безопасности, бережливость в обращении с информацией, двухфакторная аутентификация, мониторинг активности, политики и процедуры безопасности, сотрудничество, обмен опытом, чрезвычайные ситуации, реагирование на инциденты, обнаружение социальной инженерии, симуляции атак, уязвимости в безопасности, пользовательская безопасность, конфиденциальная информация, социальные сети, подозрительное поведение, меры предосторожности.

# HOW TO PROTECT YOURSELF FROM SOCIAL ENGINEERING: STRATEGIES AND TACTICS

**Perevertun D.R**.
*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com*

**This article discusses one of the most urgent and dangerous threats in the field of information security - social engineering. The author provides strategies and tactics that will help both individuals and organizations to strengthen their protection against manipulation and attacks aimed at the human factor. The article focuses on the importance of training and awareness of employees, thrift in handling confidential information, the use of two-factor authentication, suspicion and constant updating of security methods. Readers will receive practical tips and instructions that will help them better protect their personal and corporate data from social engineers.**

Keywords: Social engineering, information security, manipulation, security training, thrift in handling information, two-factor authentication, activity monitoring, security policies and procedures, cooperation, exchange of experience, emergencies, incident response, detection of social engineering, attack simulation, security vulnerabilities, user security, confidential information, social networks, suspicious behavior, precautions.

Социальная инженерия - это искусство манипуляции людьми с целью получения доступа к конфиденциальной информации или выполнения вредоносных действий. Хотя технологии информационной безопасности совершенствуются, люди по-прежнему остаются наиболее уязвимым звеном в цепи безопасности. В этой статье мы рассмотрим стратегии и тактики, которые помогут вам защититься от социальной инженерии и укрепить вашу информационную безопасность.

**1. Обучение и осведомленность**

Самый важный шаг в защите от социальной инженерии - это обучение и осведомленность сотрудников и пользователей. [1-2] Поддерживайте регулярные тренировки и обучение по вопросам безопасности, чтобы люди могли узнавать потенциальные атаки. Обучение должно включать в себя следующие аспекты:

- Идентификация типичных методов социальной инженерии: фишинг, бэйтинг, проникновение под прикрытием и другие.
- Правила безопасности для обработки электронной почты и веб-сайтов.
- Способы аутентификации и проверки личности.

**2. Бережливость с информацией**

Одним из ключевых принципов защиты от социальной инженерии является осторожность в обращении с информацией. Сотрудники и пользователи должны знать, какие данные могут быть раскрыты, а какие - нет. Важные моменты включают в себя:

- Не разглашайте конфиденциальную информацию по телефону или по электронной почте без проверки личности получателя. [3-4]
- Остерегайтесь запросов на предоставление личных данных, особенно внезапных и непрошеных.
- Следите за тем, какую информацию вы размещаете на социальных сетях и в публичных источниках.
- Не разглашайте личные данные, такие как пароли и пин-коды, никому, даже сотрудникам технической поддержки, если вы не уверены в их легитимности.

**3. Двухфакторная аутентификация [5-6]**

Использование двухфакторной аутентификации (2FA) является эффективным средством защиты от социальной инженерии. 2FA требует два способа аутентификации для доступа к аккаунту, что делает его более сложным для злоумышленников. Подсказывайте пользователям и сотрудникам включить 2FA для всех своих онлайн-аккаунтов.

**4. Подозрительность**

Следите за подозрительными ситуациями и запросами. Если что-то кажется слишком хорошим, чтобы быть правдой, или вызывает сомнения, лучше перепроверьте. Не бойтесь задавать вопросы и убедитесь, что запросы на доступ к информации или финансам подлинны.

**5. Постоянное обновление**

Социальные инженеры постоянно совершенствуют свои методы. Поэтому важно постоянно обновлять свои знания и методы защиты. Следите за новыми трендами и уязвимостями, чтобы адаптировать свои меры безопасности.

**6. Мониторинг активности**

Для более эффективной защиты от социальной инженерии важно внедрить системы мониторинга активности. Эти системы могут помочь выявить необычную активность или подозрительные события, связанные с доступом к данным или аккаунтам. Мониторинг также позволяет быстро реагировать на потенциальные инциденты безопасности.

**7. Обновление политик и процедур безопасности**

Соблюдение актуальных политик и процедур безопасности является ключевым аспектом защиты от социальной инженерии. Организации и пользователи должны периодически пересматривать и обновлять свои политики безопасности в соответствии с изменяющимися угрозами и лучшими практиками. Важно также обеспечить строгое соблюдение этих политик среди всех сотрудников и пользователей.

**8. Сотрудничество и обмен опытом**

Обмен опытом и сотрудничество с другими организациями и экспертами в области информационной безопасности могут быть чрезвычайно полезными. [7] Опытные специалисты могут предоставить ценные советы и рекомендации, а также помочь идентифицировать уязвимости в системах безопасности.

**9. Чрезвычайные ситуации и реагирование**

Несмотря на все предосторожности, инциденты безопасности могут произойти. Поэтому важно иметь четко разработанные планы чрезвычайных ситуаций и механизмы реагирования. Эффективная реакция на инциденты может минимизировать ущерб и предотвратить дополнительные атаки.

**10. Обучение по обнаружению социальной инженерии**

Следует также обучать сотрудников и пользователей навыкам обнаружения социальной инженерии. Чем больше людей способны распознавать манипуляции и подозрительное поведение, тем меньше вероятность успешных атак. Проведение симуляций атак и тренировок по обнаружению социальной инженерии может быть весьма полезным.

Социальная инженерия остается серьезной и эволюционирующей угрозой информационной безопасности. Однако с правильными мерами предосторожности, обучением и практическими навыками, вы и ваша организация можете укрепить свою защиту и минимизировать риски. Защита от социальной инженерии - это постоянный процесс, и его успешное внедрение может значительно повысить безопасность в целом. Будьте бдительны и готовы к вызовам, которые может представить социальная инженерия, и обеспечьте надежную защиту своих данных и ресурсов.

**Список литературы**


1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): угрозы безопасности и конфиденциальности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н. А., Мазепин П. С., Гришин Н. А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С.152-156.
7. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //ОФТАЛЬМОХИРУРГИЯ. – 2022.–№. 4.–С.51-57.


**References**


1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N. A., Timofeev R. S. Comparison of training methods for convolutional neural networks //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. Kosov N. A., Mazepin P. S., Grishin N. A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.