УДК 004.056.53

ПСИХОЛОГИЧЕСКИЕ МЕХАНИЗМЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

А.Д. Кузьминич[1], А.П. Полищук[1], Т.А. Пулко[2]

[1]*Учреждение образования «Национальный детский технопарк», Минск, Беларусь*

[2] *Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

Аннотация. В статье представлен обзор современных исследований, раскрывающих психологические механизмы, лежащие в основе успешных атак социальной инженерии. Предложена классификация атак с точки зрения эксплуатируемых психологических механизмов. Проанализированы современные направления исследований, включая нейропсихологические исследования, роль индивидуальных и культурных различий, использование искусственного интеллекта и влияние глубоких фейков. Сформулированы практические выводы для разработки эффективных стратегий защиты, включающие обучение и повышение осведомленности, развитие критического мышления, усиление системы контроля доступа, многофакторную аутентификацию, внедрение технологий защиты и разработку протоколов реагирования на инциденты. Подчеркнута необходимость сотрудничества между психологами и специалистами по кибербезопасности для создания более комплексных и эффективных стратегий защиты.

Ключевые слова: социальная инженерия; психологические механизмы; эмоциональное воздействие; критическое мышление; информационная безопасность; манипуляции; дипфейки; киберпреступность; психологическая устойчивость; атаки на человеческий фактор.

PSYCHOLOGICAL MECHANISMS OF SOCIAL ENGINEERING

A.D. Kuzminich[1], A.P. Poleschuk[1], T.A. Pulko[2]

[1] *Educational Institution "National Children's Technopark", Minsk, Belarus*

[2]*Educational Institution "Belarusian State University of Informatics and Radioelectronics" Minsk, Belarus*

Abstract. The article provides an overview of modern research that reveals the psychological mechanisms underlying successful social engineering attacks. A classification of attacks is proposed in terms of the psychological mechanisms exploited. Modern research areas are analyzed, including neuropsychological studies, the role of individual and cultural differences, the use of artificial intelligence, and the impact of deep fakes. Practical conclusions are formulated for the development of effective defense strategies, including training and awareness raising, development of critical thinking, strengthening the access control system, multi-factor authentication, implementation of security technologies, and development of incident response protocols. The need for cooperation between psychologists and cybersecurity specialists to create more comprehensive and effective defense strategies is emphasized.

Keywords: Social engineering; psychological mechanisms; emotional manipulation; critical thinking; information security; manipulation; deepfakes; cybercrime; psychological resilience; human-factor attacks.

Введение

Социальная инженерия – это совокупность психологических и социологических приемов манипуляции человеком или группой людей с целью преодоления систем защиты информации и копирования или модификации информации ограниченного доступа. Использует не технические уязвимости, а человеческие слабости и остается одной из наиболее эффективных и опасных форм киберпреступности. Вместо сложных технических эксплойтов, социальные инженеры полагаются на манипулирование эмоциями, доверием, когнитивными предубеждениями жертв для достижения своих целей. Применяется для получения доступа к информации, недоступной/закрытой для/от значительного количества людей, для кражи паролей и их последующего использования в корыстных целях, для совершения махинаций в финансовых организациях, для общей дестабилизации работы предприятия и даже для конкурентной разведки. Целью злоумышленников чаще всего становятся люди, в возрастной группе от 26 до 50 лет. Это люди, обычно достигшие финансовой стабильности, что привлекает мошенников, которые хотят получить доступ к их денежным средствам. Увеличение онлайн-активности повышает вероятность столкновения с мошенниками, особенно в случае недостаточной осведомленности о методах защиты и безопасности в сети.

Основная часть

Существуют различные методы социальной инженерии, с помощью который может производиться атака на человека, такие как фишинг, вишинг, смишинг, Baiting и pretexting и другие. Доля успешных атак при применении различных методов мошенничества (данные за 3 квартал 2024 года) составила порядка 92 % для частных лиц и 50 % для организаций [1]. На долю Беларуси пришлось 7 % атак, направленных против членов Содружества: республика замыкает тройку стран - лидеров по количеству кибернападений. Жертвами кибератак в Беларуси чаще всего становились госучреждения (22%), промышленные предприятия (14 %), финансовые компании (11 %) и организации из сферы науки и образования (8 %). В результате деятельности мошенников происходит утрата жертвами их денежных средств и личных данных, что характерно как для отдельных граждан, так и для организаций. Поэтому банковские структуры, МВД и Следственный комитет Республики Беларусь заботятся о сохранности средств граждан. Указ Президента № 269 от 29 августа 2023 года «О мерах по противодействию несанкционированным платежным операциям» направлен на развитие стратегии, ставящей заслон онлайн-мошенникам. Согласно отчетам аналитиков компании Positive Technologies за 3 квартал 2024 года, к последствиям атак также относится утечка конфиденциальной информации, ставшая результатом 77 % и 52 % успешных атак на частные лица и организации соответственно.

Для любой системы безопасности одной из главных угроз является человеческий фактор, в частности, халатность сотрудников, неосведомленность людей по поводу действий злоумышленников, имеющих знания в социальной инженерии, а также уверенность в нынешних знаниях и системе безопасности. Халатность может проявляться в несоблюдении существующих правил безопасности о сохранении скрытой информации. Например, человек может оставить на видном месте код, которым злоумышленник может воспользоваться в дальнейшем для получения нужной ему информации, или же человек может быть недостаточно бдительным, и не заметить подозрительные действия со стороны злоумышленника.

Злоумышленник также может воспользоваться недостатком знаний о существующих угрозах, в том числе и о новых технологиях, которые позволят ему заполучить доверие человека. Примером такой технологии являются нейронные сети для генерации речи голосом определенных людей. Злоумышленник может с легкостью получить образец речи и голоса человека, просто позвонив ему по телефону или используя уже существующие записи из открытых источников, например, записи конференций и выступлений человека. В дальнейшем злоумышленник использует этот голос для замены своего. Используя мессенджеры и социальные сети, под предлогом сверки показаний счетчиков и данных из договора, направляют ссылки для установки сторонних программ, получают доступ к данным мобильного устройства. Этими уловками активно пользуются мошенники; они всегда выглядят максимально привлекательно и авторитетно, стараются найти точки соприкосновения [2].

При использовании всех вышеперечисленных уязвимостей, злоумышленник может достичь нужной цели за счет манипуляций. Основными объектами манипулятивного воздействия являются мышление (логическое, ассоциативное) и чувства человека. На логическое мышление могут воздействовать при помощи внесения хаоса в причинно-следственную цепочку. Суть в том, что в цепочке причинно-следственных связей берется какой-то определенный момент, выгодный для атакующего и дальше он рассматривается в качестве изначальной причины [2]. Также на логическое мышление можно воздействовать за счет целенаправленного искажения информации; путем замены рационального мышления на ассоциативное посредством сравнения с предыдущими событиями, действиями или качествами людей. Таким же методом достигают создания стереотипного мышления, но за счет более характерных для общества стереотипов. Основными приемами манипуляции является запугивание, создание чувства вины, давление времени и апелляция к эмоциям. Одним из самых распространенных чувств, на которое злоумышленник может воздействовать, является страх человека. Например, телефонные мошенники, притворяющиеся сотрудниками банка, могут сказать, что при условии, если человек не расскажет какую-либо информацию, то карта будет заблокирована. Еще одним из чувств для манипуляций над человеком, может быть чувство упущенной выгоды. Например, жертве мошенничества могут прислать сообщение с выгодным для человека предложением: скидки, курсы и так далее, для получения которых нужно указать определенную информацию, заплатить определенную сумму денег. Но чаще всего такие сообщения содержат ссылки с вредоносным программным обеспечением, отправляющую злоумышленнику информацию или дающую доступ к устройству. Осознание всех этих техник поможет не стать жертвой манипуляций.

Успех социальной инженерии во многом зависит от эксплуатации фундаментальных психологических принципов, которые влияют на наше поведение и принятие решений. Наиболее значимыми из них являются:

1. Принцип авторитета – социальные инженеры часто выдают себя за представителей власти (например, сотрудников полиции, налоговых органов, технических специалистов), чтобы завоевать доверие жертвы и заставить ее подчиниться.

2. Принцип взаимности – злоумышленники могут сначала предложить небольшую помощь (например, полезный совет), а затем попросить о более значительной услуге (например, предоставить конфиденциальную информацию).

3. Принцип дефицита – создание ощущения дефицита или срочности ("Только сегодня!", "Осталось всего несколько мест!") заставляет жертву действовать импульсивно, не обдумывая последствия.

4. Принцип социального доказательства – указание на то, что другие люди уже выполнили определенные действия (например, "Все наши клиенты обновили свои пароли"), может убедить жертву сделать то же самое.

5. Принцип симпатии – социальные инженеры часто стараются установить личный контакт с жертвой, проявляя дружелюбие и сочувствие.

Также важно отметить когнитивные предубеждения:

– эффект якоря (склонность чрезмерно полагаться на первую полученную информацию (якорь) при принятии решений);

– предвзятость подтверждения (склонность искать и интерпретировать информацию таким образом, чтобы подтвердить свои существующие убеждения);

– эвристика доступности (склонность переоценивать вероятность событий, которые легко вспомнить (например, события, недавно освещавшиеся в СМИ);

– эффект ореола (склонность переносить положительное впечатление об одной черте человека на другие его качества);

– эмоциональное воздействие (социальные инженеры часто используют эмоциональное воздействие, вызывая страх, тревогу, любопытство, жадность или сочувствие, чтобы дезориентировать жертву и снизить ее бдительность).

Понимание психологических механизмов, лежащих в основе атак, является ключевым элементом разработки эффективных стратегий защиты. Дальнейшие исследования в области психологии и нейронаук, а также применение искусственного интеллекта, помогут лучше понимать и предотвращать атаки социальной инженерии, делая киберпространство более безопасным для всех.

Заключение

Социальная инженерия продолжает оставаться серьезной угрозой, требующей комплексного подхода к защите. Понимание психологических механизмов социальной инженерии позволяет разрабатывать более эффективные стратегии защиты, включающие обучение и повышение осведомленности пользователей цифровой информационной среды. Растущая уязвимость пользователей перед атаками с применением социальной инженерии создает необходимость обучения сотрудников распознавать признаки фишинговых атак. Проведение регулярных тренингов для сотрудников и пользователей о различных типах атак социальной инженерии и способах их предотвращения. Важно обучать не только распознаванию технических признаков атак (например, подозрительные ссылки), но и распознаванию психологических манипуляций (например, использование авторитета, дефицита или страха), развитию критического мышления, обучая пользователей критически оценивать поступающую информацию, задавать вопросы и проверять факты. Огромное влияние могут оказать тренинги по повышению психологической устойчивости и стрессоустойчивости, что поможет пользователям любых возрастных категорий независимо от социального статуса сохранять бдительность и критическое мышление в сложных ситуациях.

В заключение, хотелось бы отметить о необходимости сотрудничества между психологами и специалистами по кибербезопасности для разработки более эффективных стратегий защиты пользователей от атак социальной инженерии в условиях сохраняющейся тенденции к стабильно высокому проценту киберпреступлений с применением различных методов мошенничества.

Список использованных источников

1. Исследование Positive Technologies: Беларусь в тройке самых атакуемых стран СНГ [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/issledovanie-positive-technologies-belarus-v-trojke-samyh-atakuemyh-stran-sng/. – Дата доступа: 10.02.2025.

2. Психологические основы социальной инженерии / Горбачев, А. В., Котенко, Е.В. // Обзор. НЦПТИ. – 2021. – № 3 (26). – С. 53 – 57.

References

1. Issledovanie Positive Technologies: Belarus' v trojke samyh atakuemyh stran SNG [Elektronnyj resurs]. – Rezhim dostupa: https://www.ptsecurity.com/ru-ru/about/news/issledovanie-positive-technologies-belarus-v-trojke-samyh-atakuemyh-stran-sng/. – Data dostupa: 10.02.2025.

2. Psihologicheskie osnovy social'noj inzhenerii / Gorbachev, A. V., Kotenko, E.V. // Obzor. NCPTI. – 2021. – № 3 (26). – S. 53 – 57.

Сведения об авторах

Кузьминич А.Д., учащаяся, учреждение образования «Национальный детский Технопарк», anastasiakzmn@mail.ru.
Полищук А.П., учащийся, учреждение образования «Национальный детский Технопарк», andrpol2008@gmail.com
Пулко Т.А., канд. техн. наук, доц., доц. каф. защиты информации, Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
pulko@bsuir.by

Information about the authors

Kuzminich A.D., student National Children's Technopark, anastasiakzmn@mail.ru.
Poleschuk, A.P., student National Children's Technopark.andrpol2008@gmail.com
Pulko T.A., PhD, Ass. Prof., Ass. Prof. of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics".
pulko@bsuir.by