

pISSN 2073-2872
eISSN 2311-875X

Угрозы и безопасность

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Андрей Леонидович ЛОМАКИН ^{a,*}, Евгений Юрьевич ХРУСТАЛЁВ ^b,
Глеб Андреевич КОСТЮРИН ^c

^a доктор экономических наук, профессор,
заведующий кафедрой экономической безопасности,
Институт права и национальной безопасности, РАНХиГС при Президенте РФ,
Москва, Российская Федерация
lomakin-al@ranepa.ru
ORCID: отсутствует
SPIN-код: 1278-4369

^b доктор экономических наук, профессор, заведующий лабораторией,
Центральный экономико-математический институт РАН (ЦЭМИ РАН),
Москва, Российская Федерация
stalev777@yandex.ru
ORCID: отсутствует
SPIN-код: 1618-1843

^c студент факультета национальной безопасности
Институт права и национальной безопасности, РАНХиГС при Президенте РФ,
Москва, Российская Федерация
g.kostyurin@yandex.ru
ORCID: отсутствует
SPIN-код: отсутствует

* Ответственный автор

История статьи:

Рег. № 602/2020
Получена 26.10.2020
Получена в
доработанном виде
13.11.2020
Одобрена 30.11.2020
Доступна онлайн
14.01.2021

УДК 004.942

JEL: F52, H56, J28, M15,
N10

Аннотация

Предмет. В связи со стремительной цифровизацией социально-экономических отношений в обществе неминуемо растет количество киберпреступлений, субъекты которых успешно применяют методы социальной инженерии. Для того чтобы эффективно предупреждать возникающие угрозы информационной безопасности личности необходимо знать основные методы социальной инженерии, а также меры безопасности по минимизации последствий возникающих угроз.

Цели. Анализ и выявление возникающих угроз информационной безопасности, связанных с социальной инженерией. Определение основных рекомендаций по предупреждению угроз и совершенствованию уровня защищенности личности от методов социальной инженерии.

Методология. В работе использованы методы системного анализа, синтеза, аналогии и обобщения.

Результаты. Выявлены наиболее распространенные инциденты, связанные с социальной инженерией, создающие угрозы информационной безопасности личности и возможные

последствия реализации данных угроз. Определены рекомендации по совершенствованию уровня защищенности личности от методов социальной инженерии как угрозы информационной безопасности.

Ключевые слова:

социальная инженерия,
информационная
безопасность,
киберугрозы

Выводы. В целях минимизации вероятности реализации угроз информационной безопасности, связанных с социальной инженерией, следует применять комплексный подход, состоящих из двух направлений. Первое направление – техническое совершенствование системы обеспечения информационной безопасности, включающее в себя всевозможные системы защиты информации, антивирусные, антифишинговые системы. Второе – повышение осведомленности личности по вопросам обеспечения информационной безопасности. В рамках данного направления государству, руководителям различных ведомств, директорам государственных и частных компаний необходимо создавать комплексную систему обучения всех граждан страны, государственных служащих, работников предприятий основам информационной безопасности.

© Издательский дом ФИНАНСЫ и КРЕДИТ, 2020

Для цитирования: Ломакин А.Л., Хрусталёв Е.Ю., Костюрин Г.А. Социальная инженерия как угроза финансовой безопасности личности // Национальные интересы: приоритеты и безопасность. – 2021. – Т. 17, № 1. – С. 150 – 166.
<https://doi.org/10.24891/ni.17.1.150>

Современные технологии стремительно упрощают жизнь человека, удовлетворяя все возрастающие потребности людей. Появление интересов человека в сфере информационных технологий неминуемо порождает возникновение угроз данным интересам. Чем больше человек использует в своей жизни IT-технологии, тем более он становится зависимым от них, и тем большими становятся риски, связанные с информационной безопасностью [1]. Для того чтобы минимизировать вероятность возникновения угроз информационной безопасности личности, необходимо применять превентивные меры защиты. В современном обществе каждый человек должен сам заботиться о своей «цифровой гигиене», и в связи с этим чрезвычайно важно постоянно обучаться, соблюдать бдительность и быть в курсе современных угроз в сфере информационной безопасности [2–5].

В XX в. хищение денежных средств и другие серьезные преступления все реже происходят в реальном мире, но гораздо чаще – в цифровом пространстве. По данным аналитического отчета Group IB за 2018 г.¹, 80% денежных средств клиентов российских банков похищаются при помощи методов социальной инженерии. В обзоре Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка

¹ Аналитический отчет Group IB – Hi-Tech Crime Trends, 2018.
URL: <https://group-ib.ru/media/hi-tech-crime-trends-2018/>

России указано, что 49% атак на организации кредитно-финансового сектора осуществляется при помощи методов социальной инженерии². Этот факт подтверждает то, что самым уязвимым звеном в цепочке обеспечения информационной безопасности является человек (*рис. 1*).

Социальная инженерия – это совокупность методов манипуляции действиями человека в целях получения необходимого доступа к информации. Основная цель социальной инженерии – получение доступа к информации, банковским данным, защищенным системам.

Для того чтобы предпринимать меры по обеспечению безопасности от воздействия методов социальной инженерии, необходимо знать ее основные методы и способы защиты от них.

Компанией Positive Technologies в 2018 г. проводилось исследование³ на основе 3 000 отправленных писем, содержащих ссылки на веб-ресурсы, формы для ввода логинов/паролей и приложенные файлы. Самым успешным типом социальной инженерии оказался фишинг (подмена реальных веб-страниц фальшивыми): 27% сотрудников различных компаний перешли по данной ссылке. Чаще всего пользователи не глядя переходят по ссылкам, попадая на вредоносный интернет-ресурс. Однако когда пользователю предлагается скачать файл и запустить его, то на каждом следующем шаге вероятность успеха кибератаки снижается. Именно поэтому только 7% сотрудников скачали файл, приложенный к письму (*рис. 2*). Исследование показало, что в 88% случаев в переписку вступают сотрудники, не являющиеся IT-специалистами⁴, а каждый четвертый сотрудник являлся руководителем отдела.

Также интересно то, что среди тех, кто пошел на контакт со злоумышленниками, были и специалисты по информационной безопасности компаний, что в очередной раз подтверждает высокую эффективность и работоспособность методов социальной инженерии (*рис. 3*).

Далее приведем примеры случаев, связанных с социальной инженерией и создающих угрозы информационной безопасности личности в российской практике, а также рекомендации по нейтрализации возникающих угроз.

² Обзор основных типов компьютерных атак в кредитно финансовой сфере в 2018 г. / Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Департамента информационной безопасности Банка России.
URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf

³ Аналитический отчет Positive Technologies – Positive Research, 2018.
URL: <https://ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/>

⁴ Пацация С.Б. Проблемы кибер-рисков в современности: материалы международной научно-практической конференции «Новая наука как результат инновационного развития общества». Уфа: ООО «Агентство международных исследований», 2017. С. 111–113; Саблукова Ю.Г. Классификация кибер-рисков в эпоху цифровой экономики: материалы XIX международной научно-практической конференции «Страхование в эпоху цифровой экономики: проблемы и перспективы». Йошкар-Ола: Изд-во МарГУ, 2018. С. 87–91.

Электронное письмо от неизвестного адресата. В письме требуют в срочном порядке подписать договор или согласовать какой-либо акт (рис. 4). Есть вероятность, что вложенный файл заражен вирусом, поэтому ни в коем случае нельзя переходить по ссылкам и открывать вложенные файлы. Необходимо направить письмо в отдел информационной безопасности для проверки.

Электронное письмо от доверенного адресата. Например, бухгалтеру организации приходит письмо от адресата, с которым ранее уже была коммуникация. В письме могут требовать срочно оплатить задолженность или подписать договор. Есть вероятность, что данный почтовый ящик был взломан, поэтому рекомендация, данная ранее, уже не работает.

В данном случае не стоит торопиться открывать файл, а следует поинтересоваться, о каком договоре идет речь, уточнить условия договора. Если письмо было отправлено злоумышленниками, то чаще всего ответа не поступит, поскольку такого рода рассылка не предполагает обратной связи. В данной ситуации цель злоумышленника – клик по ссылке или открытие вредоносного файла, а не коммуникация с объектом атаки.

Замаскированные ссылки. На электронную почту поступает сообщение, где указано, что сайт организации объекта атаки не работает, прилагается ссылка на скриншот. Видимая ссылка действительно содержит скриншот, однако в действительности переход осуществляется по другой ссылке, замаскированной под данную (рис. 5).

Прежде чем осуществлять переход по любой ссылке необходимо сверить ее с действительной ссылкой, которую можно увидеть в левом нижнем углу сайта при наведении курсора на видимую ссылку.

Необычное поздравление от необычной компании. Предварительно злоумышленниками создается сайт с редким названием компании и доменным именем для того, чтобы он находился на первом месте в поисковой выдаче при соответствующем запросе. Сотрудникам компаний на электронную почту отсылается поздравление с праздником от компании с необычным, уникальным названием (рис. 6). Многим объектам кибератаки становится интересно узнать о данной компании, соответственно, они вводят в поисковую систему название и попадают на сайт, содержащий вредоносный код.

Всегда необходимо проверять, были ли взаимодействия с данной компанией ранее, и воздержаться от поиска информации о подозрительных кампаниях в Интернете.

«Подписка успешно активирована!». На электронную почту приходит уведомление об успешно активированной подписке на рассылку ненужной вам информации (регулярная отправка прайс-листа с железобетонной

продукцией). После нажатия на кнопку отписки от рассылки есть вероятность перехода на зараженный интернет-ресурс (рис. 7).

Данные письма следует игнорировать и отправлять в раздел «Спам».

Персональный вирус. Персонализированная рассылка прайс-листов, каталогов, справочной информации по тематикам, интересующих жертву кибератаки (рис. 8).

Для того чтобы убедиться в безопасности вложенных файлов, необходимо не скачивать их на компьютер, а открыть через сервисы Яндекса или Mail.ru, интегрированные в почтовый сервис. В случае, если открытие на удаленных компьютерах Яндекса или Mail.ru не произошло – значит, файл был заражен.

Самостоятельный поиск ловушки. Согласно статистике Яндекса, поисковый запрос «Сбербанк онлайн скачать» вводят в поисковую строку более 100 000 пользователей в месяц. Злоумышленники, воспользовавшись таким спросом, создают рекламную кампанию в Яндекс.Директ (реклама в поисковой выдаче Яндекса), выдвигая свой сайт, похожий на официальный сайт «Сбербанка», на первую позицию в поисковой выдаче. Пользователь переходит на сайт, думая, что это официальный сайт «Сбербанка», однако это не так. После прохождения регистрации на таком сайте пользователь самостоятельно передает данные своей банковской карты злоумышленникам (рис. 9).

Всегда необходимо проверять доменное имя сайта, на который вы собираетесь зайти, кроме того, сайт должен в большинстве случаев находиться в органической выдаче Яндекса, а не в платном размещении.

Звонок из «Сбербанка». Мошенником осуществляется звонок, в котором он, представляясь сотрудником «Сбербанка», сообщает, что банковский счет объекта атаки заблокирован в связи с мошенническими действиями третьих лиц, и необходимо срочно предотвратить данную угрозу, сообщив конфиденциальную информацию сотруднику.

В данном случае необходимо немедленно прекратить разговор и перезвонить по официальному номеру банка, указанному на оборотной стороне банковской карты.

Звонок «случилась беда». Данные звонки чаще всего более тщательно персонализируются, чем звонки из «банков». Мошенник сообщает, что ваш сын/дочь попал в ДТП (находится в больнице и др.), и необходимо срочно для возмещения ущерба (оплаты операции) перевести некоторую сумму денег.

Самое главное в данной ситуации – не впадать в панику. Необходимо закончить разговор и связаться с самим человеком или людьми, которые могут быть рядом с ним сейчас.

Двойник в социальной сети. Мошенником выбирается жертва – аккаунт в социальной сети и создается точно такой же аккаунт, с аналогичным описанием, фотографиями и прочей информацией. Происходит массовая рассылка друзьям жертвы с просьбой дать взаймы некоторую, вполне доступную сумму. Данный метод жизнеспособен лишь потому, что пользователи, увидев идентичное название аккаунта и фотографию, сразу идентифицируют его, не переходя на страницу профиля.

Необходимо всегда проверять страницы на предмет двойника, и даже если аккаунт подлинный, не спешить отправлять деньги. Обязательно свяжитесь с человеком по другим каналам связи, чтобы окончательно убедиться в том, что просьба исходит именно от него.

Злоумышленники всегда будут использовать методы социальной инженерии по причине их высокой эффективности и дешевизны. Эффективность таких методов обусловлена тем, что человек является самым уязвимым элементом в системе обеспечения информационной безопасности [6, 7]. Для снижения негативного воздействия человеческого фактора на систему обеспечения информационной безопасности необходимо проводить регулярное обучение сотрудников компаний, государственных служащих, а также всех людей, осуществляющих взаимодействие с современными информационными системами⁵ (табл. 1).

К сожалению, угрозы информационной безопасности, связанные с социальной инженерией, не могут быть уничтожены до тех пор, пока субъектом принятия каких-либо решений является человек. Однако возможно минимизировать вероятность реализации данных угроз [8, 9].

В целях минимизации вероятности реализации угроз информационной безопасности, связанных с социальной инженерией, необходимо применить комплексный подход, состоящих из двух направлений. Первое направление – это техническое совершенствование системы обеспечения информационной безопасности, включающее в себя всевозможные способы защиты информации, антивирусные, антифишинговые системы. Данное направление быстро развивается, и на данный момент существуют системы, удовлетворяющие практически всем условиям информационной защищенности. Второе направление – повышение осведомленности

⁵ Полетыкин А.Г. Методика оценки киберустойчивости: материалы VII международной конференции «Управление развитием крупномасштабных систем (MLSD'2013)». М.: Институт проблем управления им. В.А. Трапезникова РАН, 2013. С. 193–200; Гришин М.Н. Кибербезопасность. Средства и методы криптографической защиты информации: материалы XIX региональной научно-практической конференции «Молодежь XXI века: шаг в будущее». Благовещенск: Изд-во АмГУ, 2018. С. 175–176.

пользователей по вопросам обеспечения информационной безопасности. В рамках данного направления государству, руководителям различных ведомств, директорам государственных и частных компаний необходимо создавать комплексную систему обучения всех граждан страны, государственных служащих, работников предприятий основам информационной безопасности (ИБ). Каналами коммуникации для достижения ИБ осведомленности могут быть СМИ, бесплатные образовательные программы для граждан страны, позволяющие получить понимание об основах «цифровой гигиены», специализированные курсы и тренинги [10–13].

В сфере информационной безопасности очень четко можно увидеть работу двух жизненных правил: «Незнание не освобождает от ответственности» и «Предупрежден, значит, вооружен», что можно интерпретировать как «Осведомлен, то есть защищен». Эффективное противодействие угрозам информационной безопасности невозможно осуществить без предупредительных, превентивных мер защиты.

Таблица 1

Инциденты, создающие угрозы информационной безопасности личности, и меры нейтрализации возникающих угроз

Table 1

Incidents that pose threats to personal information security and measures to eliminate emerging threats

Инциденты, создающие угрозы ИБ	Меры нейтрализации угроз ИБ
Электронное письмо от неизвестного адресата	Не открывать вложения и не переходить по ссылкам. Сообщить службе информационной безопасности
Электронное письмо от доверенного адресата	Не открывать вложения и не переходить по ссылкам. Уточнить подробности, задать встречный вопрос
Замаскированные ссылки	Убедиться в подлинности ссылки, прежде чем совершать переход
Необычное поздравление от необычной компании	Воздержаться от поиска информации о подозрительных компаниях в Интернете
«Подписка успешно активирована!»	Игнорировать, отправить в раздел «Спам»
Персональный вирус	Не скачивать файлы на ПК. Можно открыть вложения через сервисы Яндекс/Mail.ru, интегрированные в почтовый сервис
Самостоятельный поиск ловушки	Проверить доменное имя сайта, убедиться в его подлинности
Звонок из «Сбербанка»	Немедленно прекратить разговор и перезвонить по номеру телефона банка, указанного на карте
Звонок – «случилась беда»	Не впадать в панику. Связаться с человеком и людьми, которые могут быть рядом
«Двойник» в социальной сети	Проверять страницы на предмет двойника. Связаться с человеком по другим каналам связи

Источник: авторская разработка

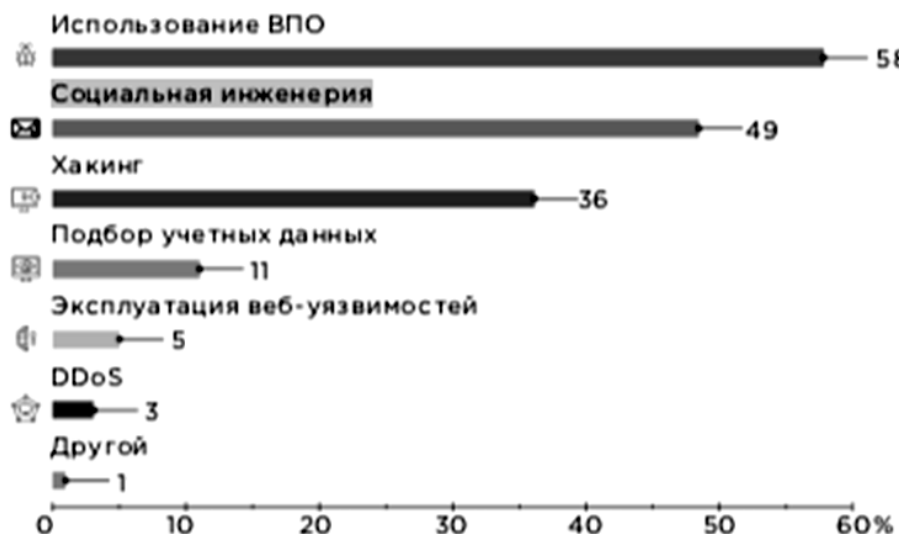
Source: Authoring

Рисунок 1

Методы атак на организации кредитно-финансового сектора

Figure 1

Methods for attacking financial sector organizations



Источник: Аналитический отчет Group IB – Hi-Tech Crime Trends, 2018.

URL: <https://group-ib.ru/media/hi-tech-crime-trends-2018/>

Source: Analytical Report of Group IB – Hi-Tech Crime Trends, 2018.

URL: <https://group-ib.ru/media/hi-tech-crime-trends-2018/>

Рисунок 2

Результативность e-mail рассылки

Figure 2

The efficiency of e-mailout



Источник: Аналитический отчет Positive Technologies – Positive Research, 2018.

URL: <https://ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/>

Source: Analytical Report of Positive Technologies– Positive Research, 2018.

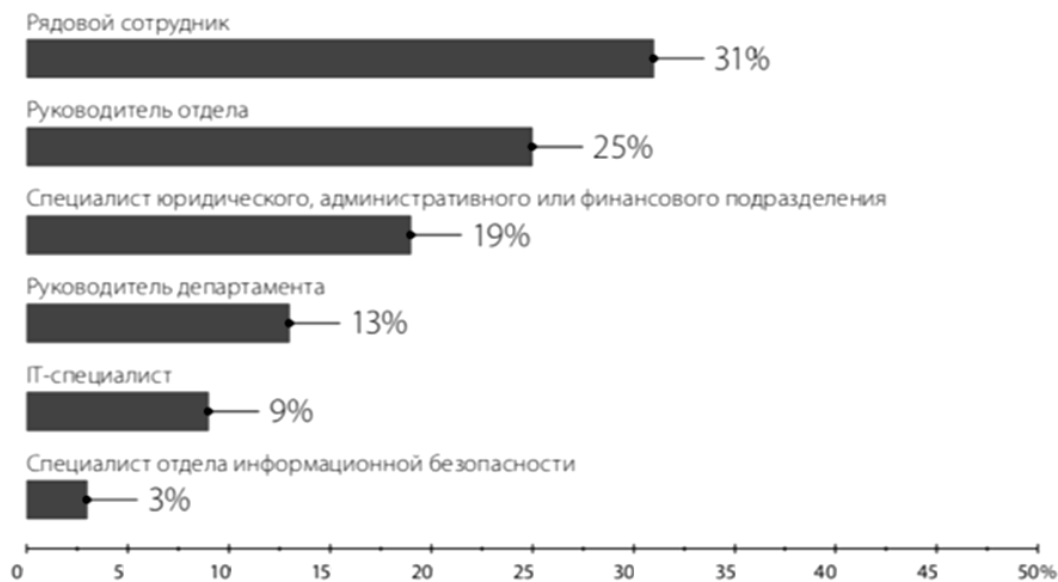
URL: <https://ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/>

Рисунок 3

Должности сотрудников, вступивших в переписку

Figure 3

Positions of employees in correspondence



Источник: авторская разработка

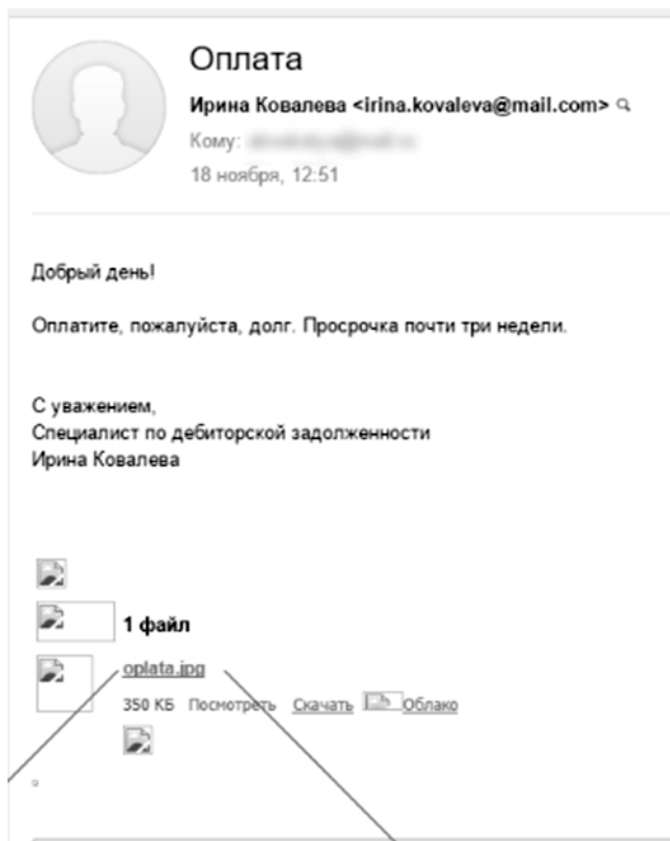
Source: Authoring

Рисунок 4

Пример электронного письма от неизвестного адресата

Figure 4

An example of an e-mail from an unknown sender

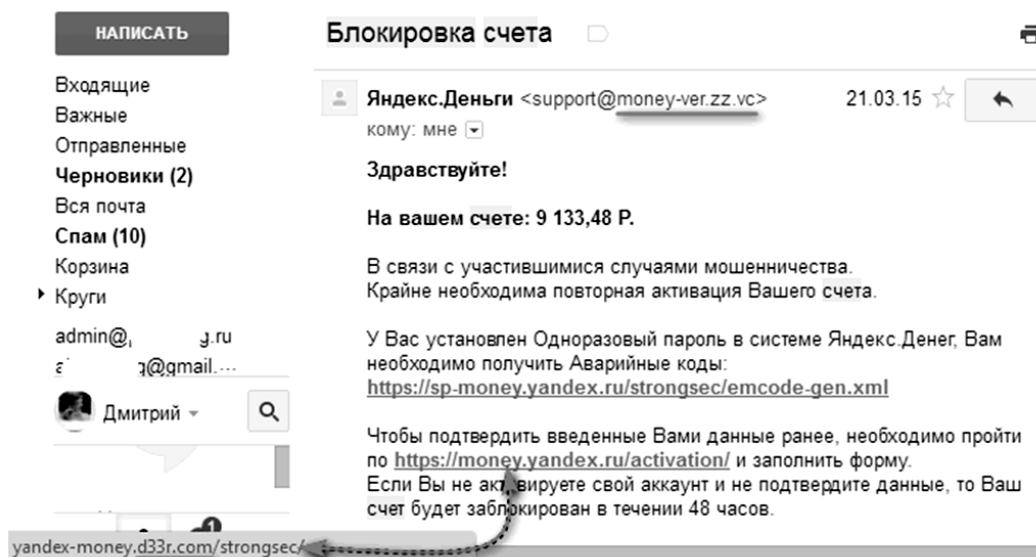


Источник: авторская разработка

Source: Authoring

Рисунок 5
Пример письма с замаскированной ссылкой

Figure 5
An example of a letter with a camouflaged link

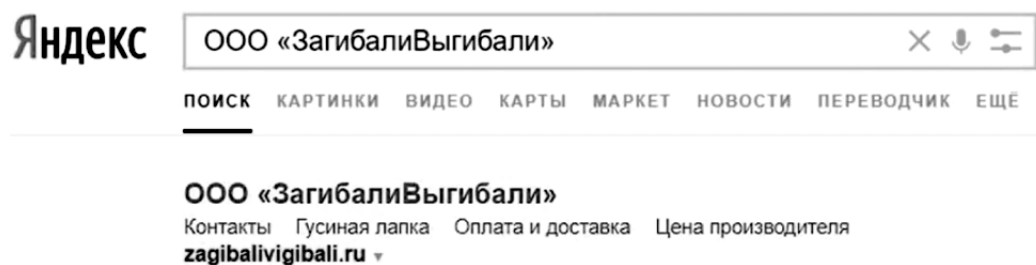


Источник: авторская разработка

Source: Authoring

Рисунок 6
Необычная компания в поисковой выдаче «Яндекса»

Figure 6
An unusual company in search results of Yandex



Источник: авторская разработка

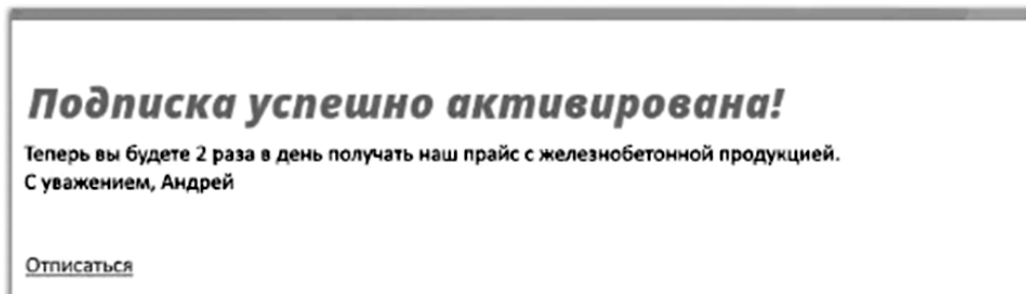
Source: Authoring

Рисунок 7

Пример письма с уведомлением об активированной подписке

Figure 7

An example of a letter with an activated subscription notification



Источник: авторская разработка

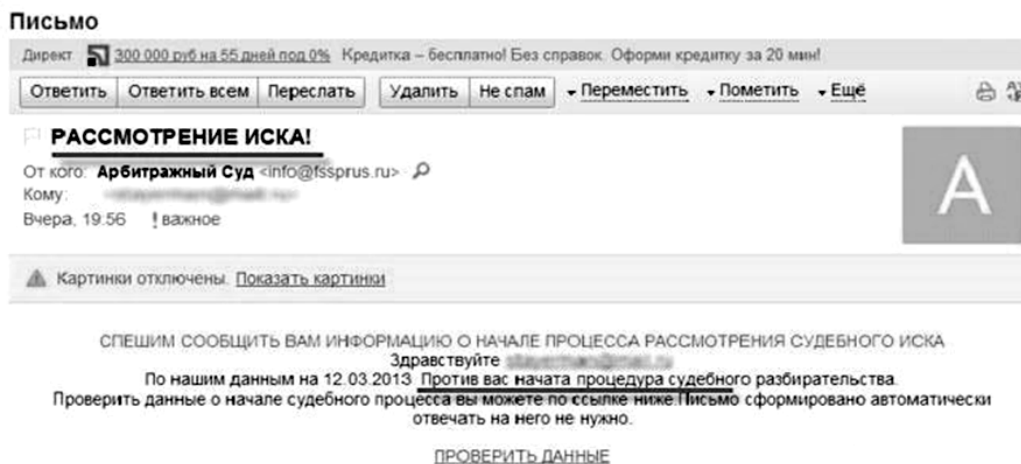
Source: Authoring

Рисунок 8

Пример персонализированной спам-рассылки

Figure 8

An example of personalized spam mailing



Источник: авторская разработка

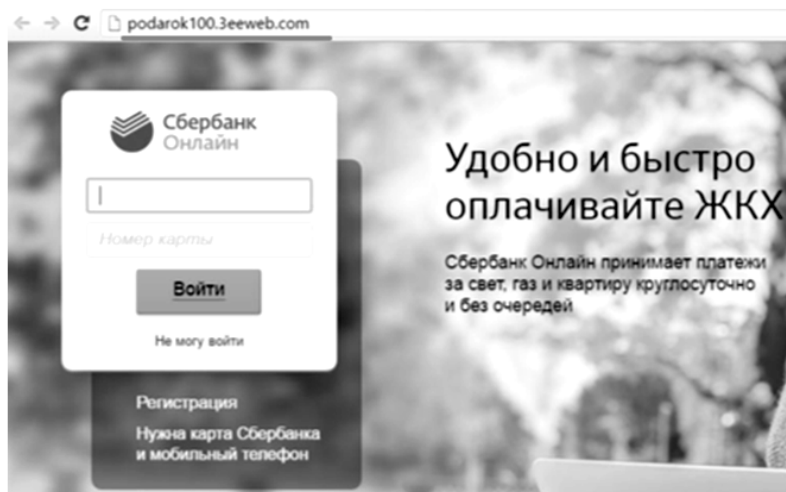
Source: Authoring

Рисунок 9

Сайт, похожий на официальный сайт «Сбербанка»

Figure 9

A website similar to Sberbank's official website



Источник: авторская разработка

Source: Authoring

Список литературы

1. Хрусталёв Е.Ю., Костюрин Г.А. Киберугрозы: причины возникновения и рекомендации по предупреждению // *Национальные интересы: приоритеты и безопасность*. 2019. Т. 15. Вып. 6. С. 1185–1194. URL: <https://doi.org/10.24891/ni.15.6.1185>
2. Бобылев А.Е., Трофимова А.В. Проблема защиты данных в Интернете вещей // *Nauka-Rastudent.ru*. 2016. № 3. С. 25. URL: <https://nauka-rastudent.ru/27/3279/>
3. Гольчевский Ю.В., Филимонова Н.А. Подход к обнаружению вредоносной активности в интернете вещей // *Информация и безопасность*. 2017. Т. 20. № 3. С. 464–467.
4. Semenova K.D., Tarasova K.I. Statistical Research of Global Cyber-Risks: The Cost of Cyber-Crime. Topical Questions of Contemporary Science Collection of Scientific Articles. Aspekt Publishing. 2017. С. 315–320. URL: <http://dSPACE.oneu.edu.ua/jspui/bitstream/123456789/5741/1/Statistical%20research%20of%20global%20cyber-risks%20the%20cost%20of%20cyber-crime.pdf>
5. Вяткин А.А. Экономическая безопасность электронных платежных систем: снижение киберрисков в условиях цифровой трансформации // *Инновационное развитие экономики*. 2018. № 5. С. 295–298.

6. Alosaimi R., Alnuem M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4, pp. 1–11.
URL: <https://doi.org/10.5121/ijcsit.2016.8401>
7. Андреев Н.О. Формирование и развитие угроз в информационных системах // Прикладная информатика. 2006. № 6. С. 87–100.
URL: <https://cyberleninka.ru/article/n/formirovanie-i-razvitie-ugroz-v-informatsionnyh-sistemah/viewer>
8. Турыгина В.Ф., Форд В.Ф., Матвеевнина А.И. Применение машинного обучения в кибер-безопасности // Научный альманах. 2017. № 6-1. С. 405–408.
9. Глотина И.М. Киберпреступность как теневой бизнес // Вестник Челябинского государственного университета. 2016. № 6. С. 51–57.
URL: <https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoy-biznes/viewer>
10. Белова И.В. Формулировка понятия «информационная безопасность» в учебном курсе дисциплины «Основы информационной безопасности» // Психология, социология и педагогика. 2011. № 3.
URL: <http://psychology.snauka.ru/2011/12/74>
11. Кадулин В.Е., Клочкова Е.Н. Соотношение понятий «кибербезопасность» и «информационная безопасность» в современном правовом поле // Вопросы кибербезопасности. 2017. № S2. С. 7–10.
12. Алпеев А.С. Терминология безопасности: кибербезопасность и информационная безопасность // Вопросы кибербезопасности. 2014. № 5. С. 39–42. URL: <https://cyberleninka.ru/article/n/terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost/viewer>
13. Гаврилова Е.А. Исследование методов обнаружения сетевых атак // Научные записки молодых исследователей. 2017. № 4. С. 55–58.
URL: <https://cyberleninka.ru/article/n/issledovanie-metodov-obnaruzheniya-setevyh-atak/viewer>

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи. Настоящее заявление относится к проведению научной работы, сбору и обработке данных, написанию и подготовке статьи, принятию решения о публикации рукописи.

pISSN 2073-2872
eISSN 2311-875X

Threats and Security

SOCIAL ENGINEERING AS A THREAT TO PERSONAL FINANCIAL SECURITY

Andrei L. LOMAKIN ^{a*}, Evgenii Yu. KHRUSTALEV ^b, Gleb A. KOSTYURIN ^c

^a Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russian Federation
lomakin-al@ranepa.ru
ORCID: not available

^b Central Economics and Mathematics Institute, Russian Academy of Sciences (CEMI RAS), Moscow, Russian Federation
stalev777@yandex.ru
ORCID: not available

^c Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russian Federation
g.kostyurin@yandex.ru
ORCID: not available

* Corresponding author

Article history:

Article No. 602/2020
Received 26 Oct 2020
Received in revised form
13 November 2020
Accepted 30 Nov 2020
Available online
14 January 2021

JEL classification: F52,
H56, J28, M15, N10

Keywords:

social engineering,
information security,
cyber threats

Abstract

Subject. As the socio-economic relationships are getting digitalized so quickly, the society faces more and more instances of cybercrime. To effectively prevent arising threats to personal information security, it is necessary to know key social engineering methods and security activities to mitigate consequences of emerging threats.

Objectives. We herein analyze and detect arising information security threats associated with social engineering. We set forth basic guidelines for preventing threats and improving the personal security from social engineering approaches.

Methods. The study relies upon methods of systems analysis, synthesis, analogy and generalization.

Results. We determined the most frequent instances associated with social engineering, which cause personal information security threats and possible implications. The article outlines guidelines for improving the persona; security from social engineering approaches as an information security threat.

Conclusions and Relevance. To make information security threats associated with social engineering less probable, there should be a comprehensive approach implying two strategies. First, the information security protection should be technologically improved, fitted with various data protection, antivirus, anti-fishing software. Second, people should be more aware of information security issues. Raising the public awareness, the government, heads of various departments, top executives of public and private organizations should set an integrated training system for people, civil servants, employees to proliferate the knowledge of information security basics.

© Publishing house FINANCE and CREDIT, 2020

Please cite this article as: Lomakin A.L., Khrustalev E.Yu., Kostyurin G.A. Social Engineering as a Threat to Personal Financial Security. *National Interests: Priorities and Security*, 2021, vol. 17, iss. 1, pp. 150–166.
<https://doi.org/10.24891/ni.17.1.150>

References

1. Khrustalev E.Yu., Kostyurin G.A. [Cyber threats: Triggers and prevention recommendations]. *Natsional'nye interesy: priority i bezopasnost' = National Interests: Priorities and Security*, 2019, vol. 15, iss. 6, pp. 1185–1194. (In Russ.) URL: <https://doi.org/10.24891/ni.15.6.1185>
2. Bobylev A.E., Trofimova A.V. [Data protection problem on the Internet of things]. *Nauka-Rastudent.ru*, 2016, no. 3, p. 25. (In Russ.) URL: <https://nauka-rastudent.ru/27/3279/>
3. Gol'chevskii Yu.V., Filimonova N.A. [Approach to detecting malicious activity on the Internet of things]. *Informatsiya i bezopasnost' = Information and Security*, 2017, vol. 20, no. 3, pp. 464–467. (In Russ.)
4. Semenova K.D., Tarasova K.I. Statistical Research of Global Cyber-risks: The Cost of Cyber-crime. In: *Topical Questions of Contemporary Science Collection of Scientific Articles*. Aspekt Publishing, 2017, pp. 315–320. URL: <http://dspace.oneu.edu.ua/jspui/bitstream/123456789/5741/1/Statistical%20research%20of%20global%20cyber-risks%20the%20cost%20of%20cyber-crime.pdf>
5. Vyatkin A.A. [The Economic Security of Electronic Payment Systems: Reducing Cyber Risks in the Conditions of Digital Transformation]. *Innovatsionnoe razvitie ekonomiki = Innovative Development of Economy*, 2018, no. 5, pp. 295–298. (In Russ.)
6. Alosaimi R., Alnuem M. Risk Management Frameworks for Cloud Computing: A Critical Review. *International Journal of Computer Science & Information Technology*, 2016, vol. 8, iss. 4, pp. 1–11. URL: <https://doi.org/10.5121/ijcsit.2016.8401>
7. Andreev N.O. [Formation and development of threats in information systems]. *Prikladnaya informatika = Applied Informatics*, 2006, no. 6, pp. 87–100. URL: <https://cyberleninka.ru/article/n/formirovanie-i-razvitie-ugroz-v-informatsionnyh-sistemah/viewer> (In Russ.)
8. Turygina V.F., Ford V.F., Matvevnina A.I. [The use of machine learning in cyber security]. *Nauchnyi al'manakh = Scientific Almanac*, 2017, no. 6-1, pp. 405–408. (In Russ.)

9. Glotina I.M. [Cybercrime as shadow business]. *Vestnik Chelyabinskogo gosudarstvennogo universiteta* = *Bulletin of Chelyabinsk State University*, 2016, no. 6, pp. 51–57.
URL: <https://cyberleninka.ru/article/n/kiberprestupnost-kak-tenevoy-biznes/viewer> (In Russ.)
10. Belova I.V. [Formulating the concept of information security in the curriculum of Fundamentals of information security]. *Psikhologiya, sotsiologiya i pedagogika* = *Psychology, Sociology and Pedagogy*, 2011, no. 3. (In Russ.) URL: <http://psychology.snauka.ru/2011/12/74>
11. Kadulin V.E., Klochkova E.N. [The relation between the concepts of information security and cyber security in the contemporary legal environment]. *Voprosy kiberbezopasnosti* = *Cybersecurity Issues*, 2017, no. S2, pp. 7–10. (In Russ.)
12. Alpeev A.S. [Terminology of insecurity: Cybersecurity, information security]. *Voprosy kiberbezopasnosti* = *Cybersecurity Issues*, 2014, no. 5, pp. 39–42.
URL: <https://cyberleninka.ru/article/n/terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost/viewer> (In Russ.)
13. Gavrilova E.A. [Research methods for detecting network attacks]. *Nauchnye zapiski molodykh issledovatelei* = *Scientific Notes of Young Scientists*, 2017, no. 4, pp. 55–58. URL: <https://cyberleninka.ru/article/n/issledovanie-metodov-obnaruzheniya-setevyh-atak/viewer> (In Russ.)

Conflict-of-interest notification

We, the authors of this article, bindingly and explicitly declare of the partial and total lack of actual or potential conflict of interest with any other third party whatsoever, which may arise as a result of the publication of this article. This statement relates to the study, data collection and interpretation, writing and preparation of the article, and the decision to submit the manuscript for publication.