

БИЗНЕС
ИДЕИ

БИЗНЕС
РЕШЕНИЯ

БИЗНЕС
ТЕХНОЛОГИИ

БИЗНЕС
ПРОЦЕССЫ

www.TOP-PERSONAL.ru

УПРАВЛЕНИЕ ПЕРСОНАЛОМ

№ 42
(550)

2019

Ведущий эксперт по управлению персоналом — 71032, 71055, 71035

Главная тема: **ЭНТРОПИЯ**



Ирина Фирсова
ПЭК

**Главное – видеть за всеми цифрами
человека, его способности
и возможность добавить энергию
в нашу команду**

Содержание

5

ЭНТРОПИЯ
Энтропия это уже последствия
Ирина Фирсова, ПЭК

11

КОМАНДА
Команда – это благо, а не наказание для сотрудников и руководства
Наталья Седых, СМП Банк

23

Трибуна HR
Трансформация может быть только одна – стратегическая
Екатерина Цыбульская, Химический концерн BASF

30

КОМАНДА
Мало создать команду, с ней еще надо постоянно работать и развивать
Анастасия Цымбал, бизнес-школа АМИ

33

КОУЧИНГ
Коучинговый стиль подразумевает управление сотрудниками через взятие ответственности за свои собственные решения
Ирина А. Иванова, ПроАктив

38

ПРИТЧА
Притча

39

КОУЧИНГ
Как идти рядом не заслоняя солнце и не пиная в спину?
Жанна Сорокина, ООО Транс Бизнес Консалтинг-Юг

43

ОБЗОР КНИГИ
Искусство обмана: социальная инженерия в мошеннических сетях
Владимир Шумков

52

КОММЕНТАРИИ
Социальная инженерия в руках мошенников весьма опасная штука и для бизнеса
Дмитрий Жирнов, «Бридж ту ЭйчАр»

56

ПО В ОФИСЕ
Штрафы за нелегальное ПО в компаниях
Анастасия Балдынова, эксперт УП

№42
(550)
Издается с 1996 г. 2019 г.

Объединенная редакция

ИД 

Издание зарегистрировано Комитетом Российской Федерации по печати. Свидетельство о регистрации выдано Министерством РФ по делам печати, телерадиовещания и средств массовых коммуникаций ПИ № 77-15375 от 12 мая 2003 г.

Официальный адрес

TR@TOP-PERSONAL.RU

Ведущие эксперты УП



Тажир Базаров



Михаил Богданов



Татьяна Ведькалова



Дмитрий Жирнов



Татьяна Коженикова



Дарья Крячкова



Виктория Петрова



Сергей Пронин

Материалы, опубликованные на данном цвете, печатаются на правах рекламы.

www.top-personal.ru

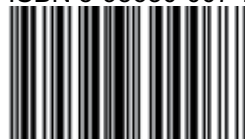
Подписано в печать 11.12.2019 г.
Формат 60x90 1/8. Печать офсетная.
Тираж 10 000 экз. Печ. л. 8.
Заказ №

Отпечатано в полном соответствии с качеством предоставленного электронного оригинал-макета в ООО «Белый ветер»
г. Москва, ул. Щипок, 28

Приглашаем авторов к сотрудничеству: tp@top-personal.ru
Издательство не несет ответственности за содержание рекламных объявлений. Издательство не всегда разделяет мнения и взгляды авторов. Рукописи не рецензируются и не возвращаются.
Цена свободная

© ООО «Журнал «Управление персоналом», 1996
© ЗАО «Бизнес-школа «Интел-Синтез», 2006

ISBN 5-95630-007-7



9 785956 300077 >

Подписные индексы
по Объединенному каталогу: 29431, 29621
ООО «МАП»: 99722
ООО «Роспечать»: 70855, 71852

Социальная инженерия в руках мошенников весьма опасная штука и для бизнеса

Но и уход в тень в Сети (когда о вас невозможно ничего найти) наносит непоправимый ущерб развитию бизнеса.

УП Какие, на Ваш взгляд, приемы социальной инженерии используются в сферах управления, образования, в психологии, в военных структурах? Можно примеры и их анализ?

 сновная цель социальной инженерии – это манипуляция людьми с целью получить от них желаемый результат. Хакер применяет социальную инженерию для того, чтобы запустить в корпоративную сеть свой вирус. Например, в моей практике был случай, когда мошенник специально «потерял» флэшку на лестнице бизнес центра, чтобы её «случайно» нашел конкретный сотрудник и из любопытства посмотрел содержимое на корпоративном компьютере, тем самым запустив «червя» в сеть. Единственная ошибка хакера, по которой его нашла служба безопасности, это то, что «червь» начал работать сразу. Утечку информа-



Дмитрий Жирнов

«Бридж ту ЭйчАр»

www.bridge2hr.ru



ции обнаружили, нашли компьютер, через который вирус попал в корпоративную сеть, опросили владельца компьютера, нашедшего флешку, посмотрели видеозаписи и вычислили жулика. Но, если бы «червь» проявил себя, например, только через месяц, то установить истинного виновника было бы практически невозможно. Даже, если сотрудник и вспомнил бы, что он подключал найденную флешку, глубина архива видеозаписей в бизнес центрах, как правило, составляет всего несколько дней. В данном примере хакер использовал любопытство как один из главных инструментов социальной инженерии.

Социальная инженерия может использоваться в любой области, где есть люди и где есть необходимость заставить их что-то сделать. Т. е. везде.

Любой инструмент можно использовать и во благо, и во зло, вспомним американский фильм «Техасская резня бензопилой» и советский фильм «Девчата».

Такие инструменты социальной инженерии, как любопытство и соревновательность широко используются в геймофикации, это один из видов обучения. Здесь эти инструменты направлены на улучшение запоминания материала и на развитие ассоциативного мышления у обучающихся.

Сфера управления персоналом – именно то поле, на котором и должен играть социальный инженер. Ведь, задача руководителя – склонить подчиненных к тому, чтобы они делали то, что нужно ему. Сами инструменты уже вторичны, кнут для рабовладельца, или демократические ценности для руководителя бирюзовой компании. В данном случае навыки социальной инженерии помогают выявить или сформировать факторы нематериальной мотивации сотрудника и использовать их для повышения эффективности труда.

Знания в сфере социальных отношений и социальной инженерии лежат и в основе вербовки агентов спецслужбами и получения доступа к секретной информации. Метод «плохой и хороший полицейский», насаждение чувства вины, демонстрация единения и взаимопомощи – это тоже инструменты социальной инженерии.

Практически, так же поступают с потребителями маркетологи, они создают заинтересованность и показывают путь как её удовлетворить – купить товар, даже если он нам и не сильно нужен.

УИ Вишинг – чем он опасен для компаний?

— Как и любой вид мошенничества, вишинг преследует цель незаконно



Эксклюзивное интервью для



Эксклюзивное интервью для



Эксклюзивное интервью для



завладеть информацией компании, а в конечном итоге её деньгами.

Но самая большая опасность вишинга заключается в том, что сотрудник, ставший невольным проводником вишинга в компанию, когда осознает, что он наделал и какой ущерб нанес компании, в большинстве случаев не идет с повинной к руководителю, а всячески саботирует и препятствует расследованию, и таким образом становится соучастником мошенника, так же не желая, что бы истина раскрылась. Он понимает, если схема мошенничества раскроется, то в лучшем случае его будут считать не самым умным человеком и он потеряет работу, в худшем – его будут судить.

УП Как сотрудникам донести серьезность сохранения информации вплоть до имени компании?

— Как и в любом другом вопросе, в случае сохранения корпоративной информации есть два варианта взаимодействия с сотрудниками: первый – это страх наказания за нарушение, или второй вариант – развить у сотрудников ощущение причастности к компании – «это моё и я никому не отдам». Но если когнитивные способности мошенника и его навыки в социальной инженерии будут выше, чем у конкретного сотрудника компании, которого он выберет своей жертвой, то никакой вариант не спасет. Для

реализации первого варианта разработывают локальные политики безопасности и NDA, и доводят под роспись до каждого сотрудника. Но, не стоит ждать от всех сотрудников ежедневного соблюдения регламента по безопасности. Компании применяют кардинальные технические меры безопасности: блокируют USB-порты и почтовые протоколы передачи данных на корпоративных компьютерах, т.е. пытаются исключить техническую составляющую вишинга и фишинга, если мошенникам все же удастся найти и использовать подходящего для их целей сотрудника компании. Если бы такие технические мероприятия были реализованы в примере, о котором я говорил в начале интервью, то найденную на лестнице флешку, корпоративный компьютер просто бы не смог загрузить.

УП Болтун – находка для шпиона!! Как бы Вы сегодня трансформировали эту мысль?

— Никак. Я бы сказал, что этот советский афоризм уже не актуален. Сейчас в интернете столько наших цифровых следов и следов наших компаний, что дополнительно сообщать шпиону или хакеру практически нечего, только пароли и пин-коды. Паспортные данные, СНИЛС, номер машины и вся остальная информация о вас бесплатно лежит в интернете.

Парадоксальная мысль: если в сегодняшних условиях пытаться ограничить информацию о себе в интернете, то ты окажешься в проигрыше. Клиенты будут находить конкурентов, а не тебя. Бизнес строится на том, что ты максимизируешь поток информации о себе, или своей компании во внешнюю среду, чтобы получить блага этой информационной среды.


 Как на практике стоит использовать мысли автора книги?

— Специалистов по информационной безопасности в ВУЗах учат тому, что совершенных систем защиты информации априори не может быть, т. к. невозможно исключить человеческий фактор. Например, банки разработали двухфакторную систему аутентификации для подтверждения финансовых операций с использо-


ванием СМС. При этом мошенник, используя социальную инженерию и купюру в 1000 рублей с помощью девушки-оператора салона сотовой связи получает дубликат вашей SIM-карты. И прощай все разработки банковских айтишников.

Предупрежден, значит вооружен. Благодаря подобным книгам, мы узнаем методы социальной инженерии и каким образом их используют мошенники. Обладая этими знаниями, мы не позволим мошенникам собой манипулировать.

***Дмитрий Жирнов,**
руководитель Кадрового агентства
Bridge2HR
www.bridge2hr.ru

Эксклюзивно для 



 приглашает HR-практиков, у кого есть интересный опыт и знания поделиться мыслями о секретах и технологиях бизнеса по теме журнала. Пишите нам – tp@top-personal.ru