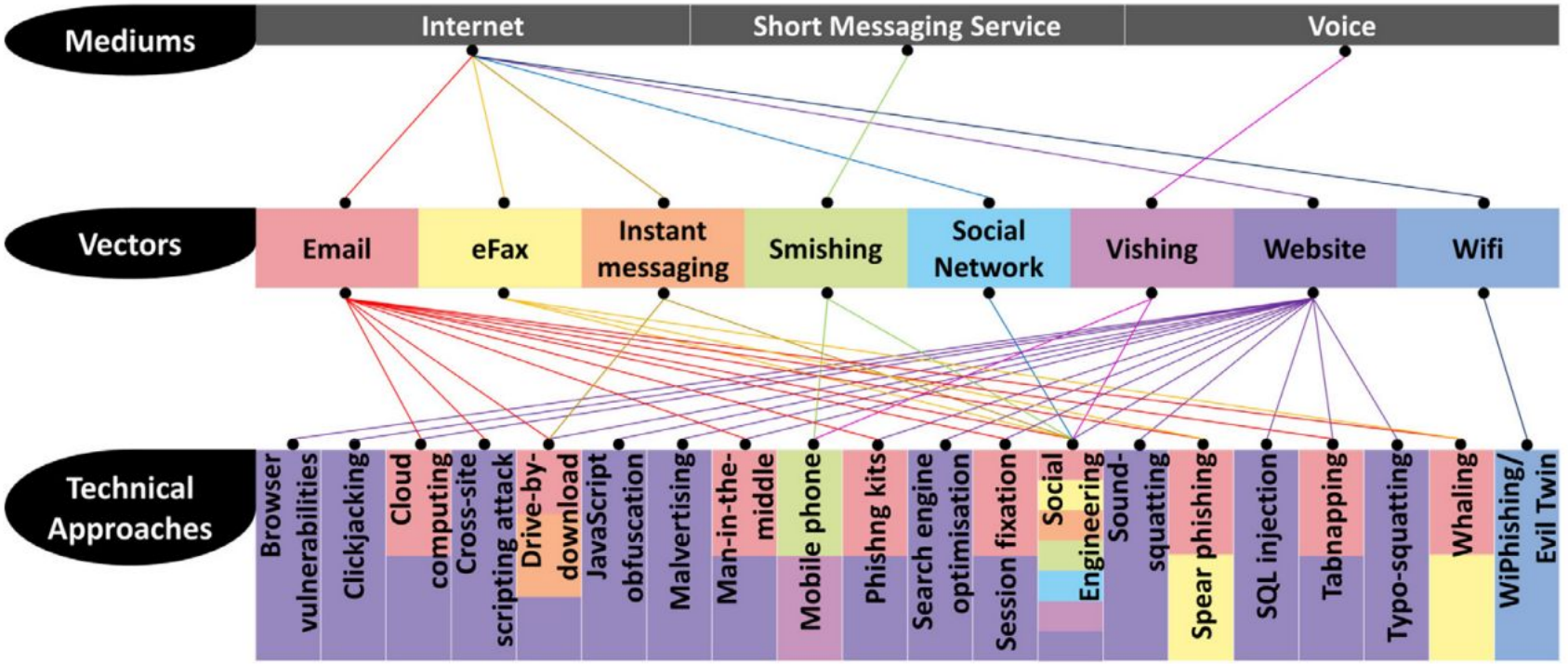
Сравнение средств и методов выявления и защиты от фишинговых атак

Коневши Р.Н.

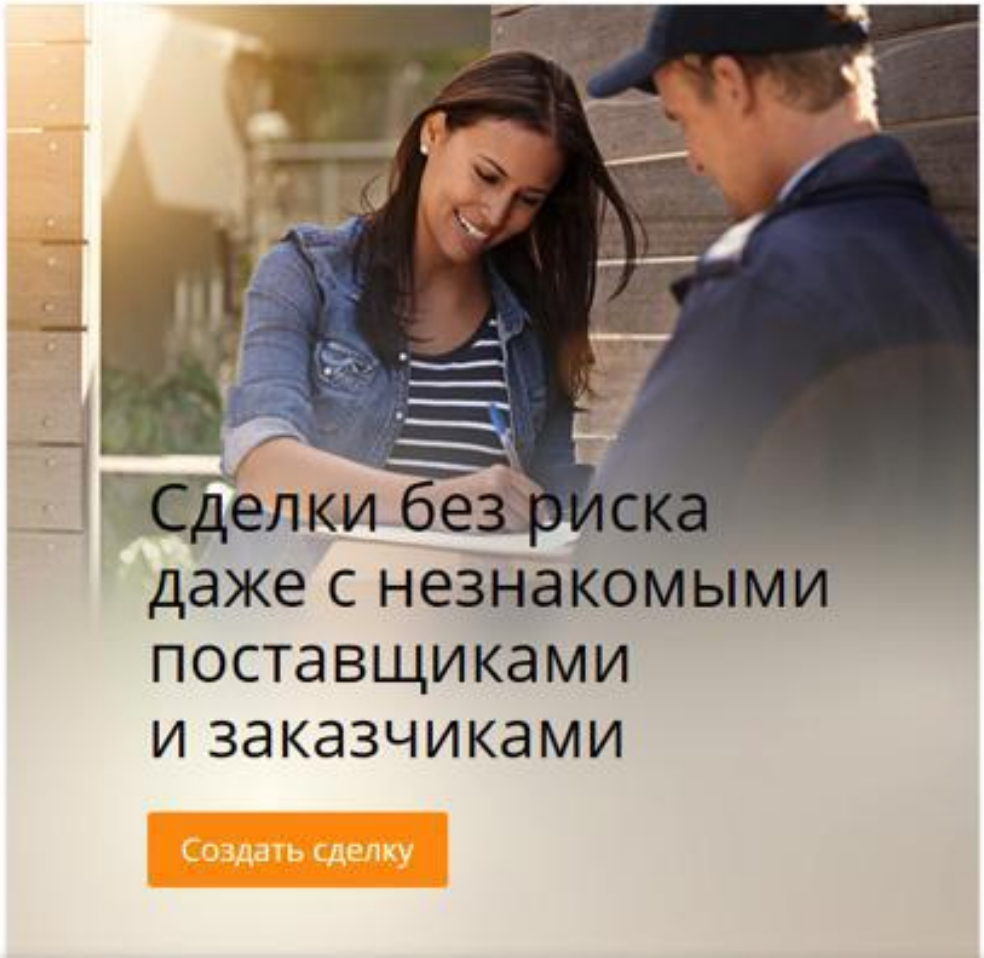
Что это?

Фишинг - один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт. В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

Что это?


Mediums
Internet
Short Messaging Service
Voice
Vectors
Email
eFax
Instant messaging
Smishing
Social Network
Vishing
Website
Wifi
Technical Approaches
Browser vulnerabilities
Clickjacking
Cloud computing
Cross-site scripting attack
Drive-by-download
JavaScript obfuscation
Malvertising
Man-in-the-middle
Mobile phone
Phishng kits
Search engine optimisation
Session fixation
Social Engineering
Sound-squatting
Spear phishing
SQL injection
Tabnapping
Typo-squatting
Whaling
WiPhishing/ Evil Twin

Сервис «Безопасная сделка»



Надежная защита продавца и покупателя

Ваши средства будут сохранены на специальном счете до исполнения обязательств по договору

Быстрое оформление

Все сделки проводятся в режиме онлайн

Выгодные условия

Комиссия за сделку всего 1,45% от суммы договора

СБЕРБАНК
Всегда рядом

Малому бизнесу и ИП | 0321 | 8 800 555-5777 | Обратная связь | Отделения и банкоматы | + Открыть счет

Главная | Лицензия | Сделка | Кредиты и гарантии | Онлайн-Сервисы | Депозиты и инвестиции

Надежная защита продавца и покупателя

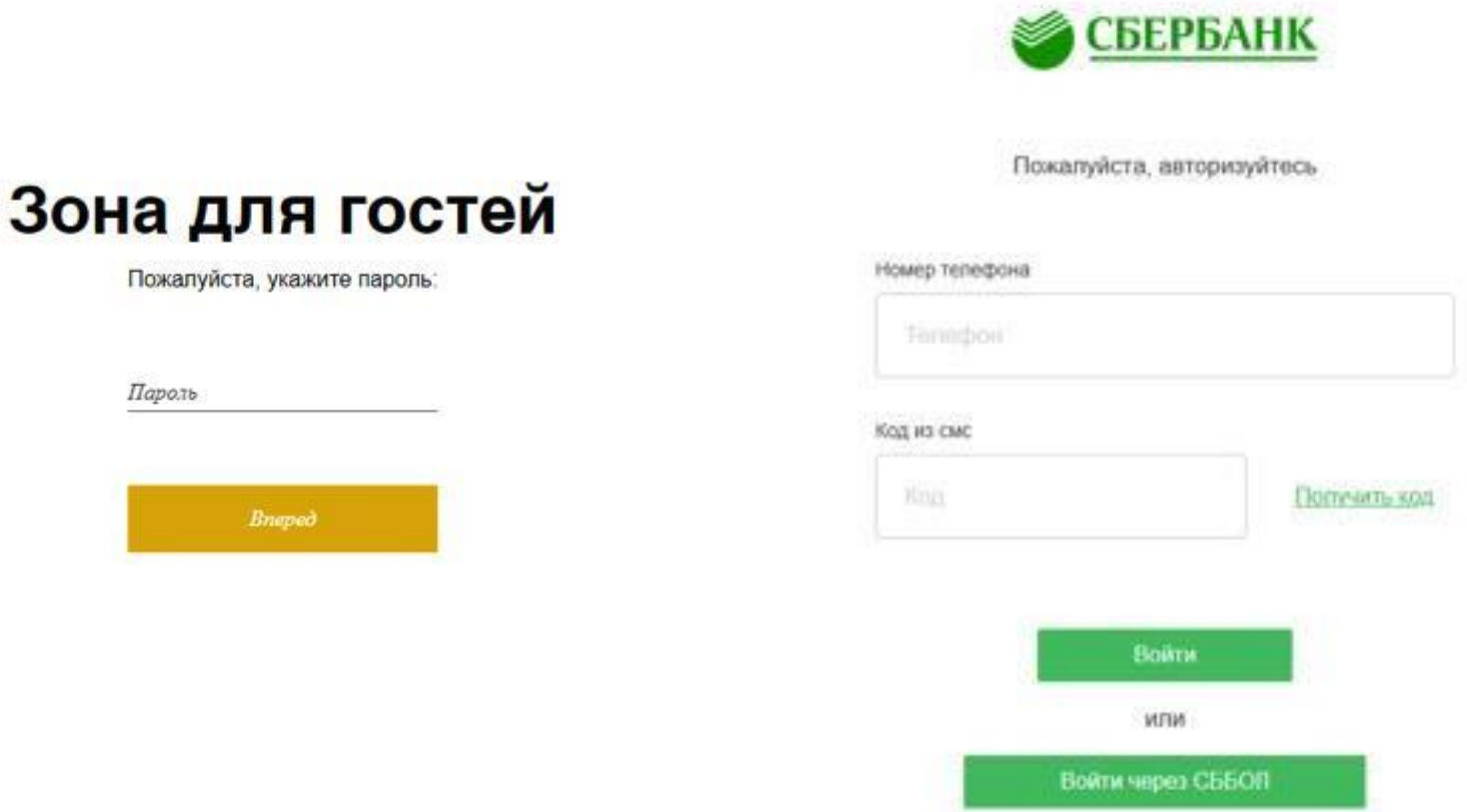
Ваши средства будут сохранены на специальном счете до исполнения обязательств по договору.

Быстрое оформление

Все сделки проводятся в режиме онлайн.

Выгодные условия

Комиссия за сделку всего 1,45% от суммы договора.


Зона для гостей
Пожалуйста, укажите пароль:
Пароль
Вперед
СБЕРБАНК
Пожалуйста, авторизуйтесь
Номер телефона
Код из смс
Получить код
Войти
или
Войти через СББОЛ

Зачем выявлять?

- Защитить личные данные пользователя (данные карт, ПДн, связки логин/пароль и т. д.)
- Защитить данные организации
- Не все фишинговые атаки используют вирусы

Что рассматриваем?

- «Классичесский» метод
- Метод без использования средств автоматизации
- Алгоритм под кодовым названием «Phishing Destroyer»

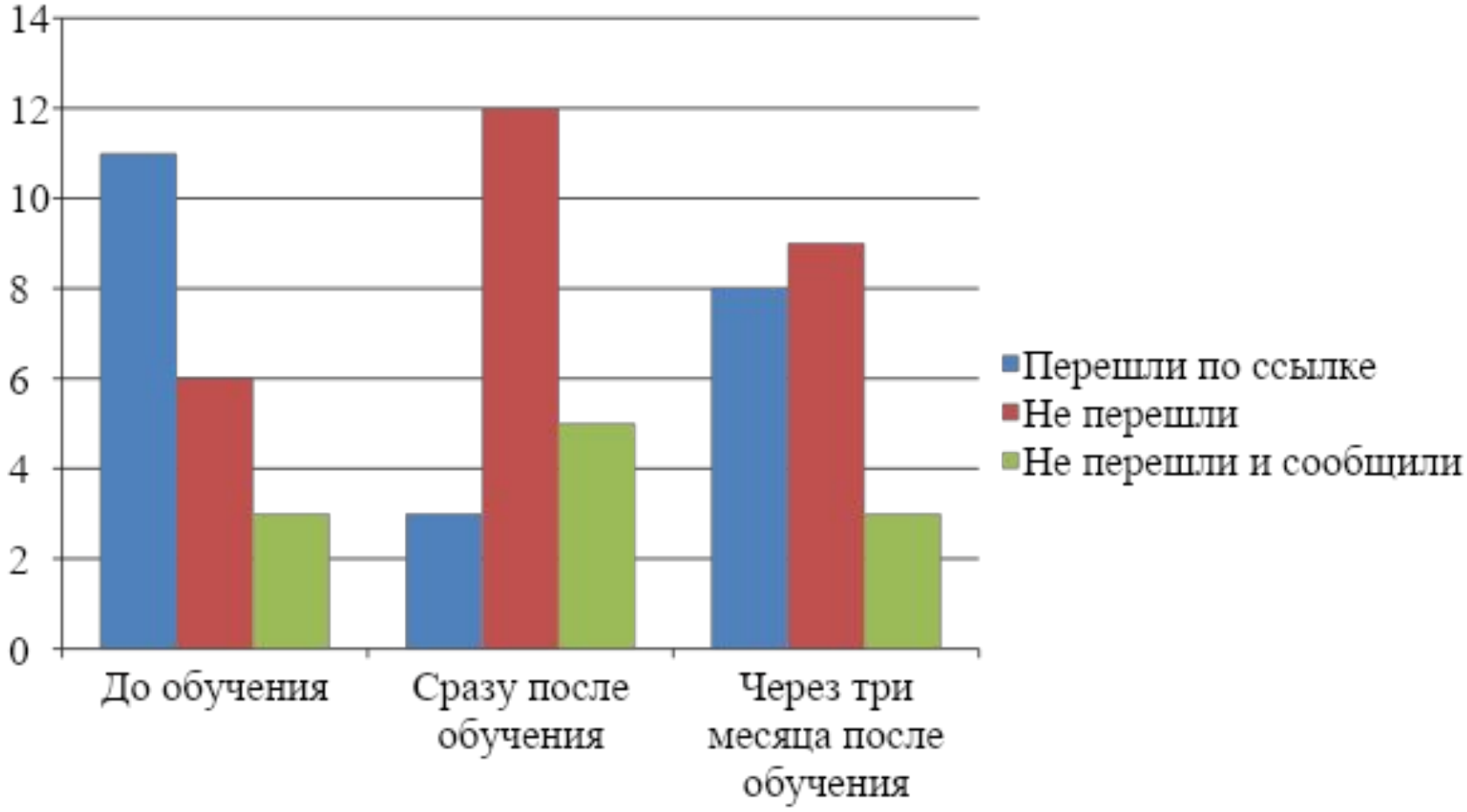
«Классический» метод

- Проверка ссылок на вредоносность
- Проверка отправителя
- Проверка совпадения реального адреса отправителя с отображаемым

Метод без использования средств автоматизации

- Обучение
- Информирование
- Тестирование

Метод без использования средств автоматизации



«Phishing Destroyer»

- Анализ текста сообщений
- Выявление общей маски фишинговых сообщений
- Использование обучения

Как работает?

- На этапе обучения составляется матрица весов связей слов
- При повторении связи вес пересчитывается как мат ожидание имеющегося значения и нового
- На этапе анализа сообщения составляется матрица связей слов и сравнивается в с текущей матрицей
- Процент совпадения весом приводится как процент вероятности фишинга

Проблемы

- Необходимость большой обучающей выборки
- Ошибки первого рода

Спасибо за внимание