

[*] SECURE-T

AT Consulting

softline®

FBK | CS
cybersecurity



БАСТИОН

Тема презентации:
Фишинг и его последствия - кейсы
и как бороться

Никишкин Харитон Григорьевич
Co-founder, CBDO, Secure-T



Вступление



Цитата |

“Требуется 20 лет для того, чтобы построить репутацию компании и всего 3 минуты инцидента по информационной безопасности для того, чтобы все это разрушить”



Стивен Наппо

Вице-президент, глава отдела
информационной безопасности
Росбанк (Societe Generale)

Проблема |

- * Большинство технически не подкованных сотрудников не знают основ цифровой гигиены, поэтому халатно относятся к информационной безопасности при использовании личных и корпоративных устройств
- * У руководителей отсутствует возможности контролировать уровень знаний своих сотрудников
- * Нельзя проверить действия сотрудников в ситуациях, приближенных к реальной атаке
- * У руководителей нет подробной аналитики по уровню подготовки сотрудников и степени их уязвимости к действиям злоумышленника



Соответствие законодательству

* Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ

- п.6 ч.1 ст.18.1 ФЗ-152: ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.



* Положения Банка России (№ 683-П, № 757-П) + ГОСТ Р 57580.1-2017

- п. 8.3.1 ГОСТ Р 57580.1-2017: обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации; повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.



* Приказ ФСТЭК России от 25 декабря 2017 г. № 239 КИИ

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости:

- Информирование и обучение персонала (ИПО)



РЫНОК

2



Статистика |

Совокупный объём данных, скомпрометированных в результате внутренних утечек, в 2019 году составил 9,87 млрд записей. Впервые это число, превысило аналогичный показатель для утечек внешних (в 2019 году в результате внешних утечек скомпрометировано 4,7 млрд записей).



Объём данных, скомпрометированных в результате внутренних утечек. Млн записей, 2013–2020 гг.

Источник: InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя.

Статистика |

Злонамеренный нарушитель редко покушается на пользовательские данные. Когда это происходит, объём похищенной информации будет сравнительно небольшим – только действительно ликвидные сведения.



Объём данных, скомпрометированных в результате умышленных утечек. Млн записей, 2013–2020 гг.

Источник: InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя.

Статистика |

Количество фишинговых атак во время карантина выросло в 4 раза.

Средний ущерб от утечки данных

4,24 млн \$

Средний объём утечки составляет

25 575

пользовательских записей

Средний ущерб от одной потерянной записи

180 \$

Источник: IBM Security. Cost of data breach report 2021

Кейсы

3



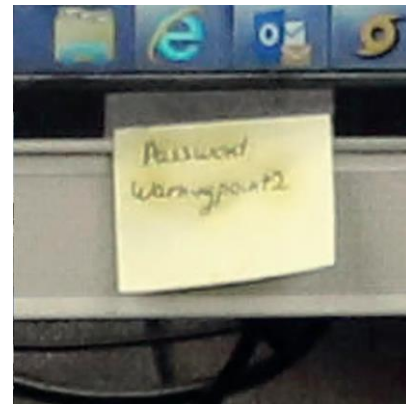
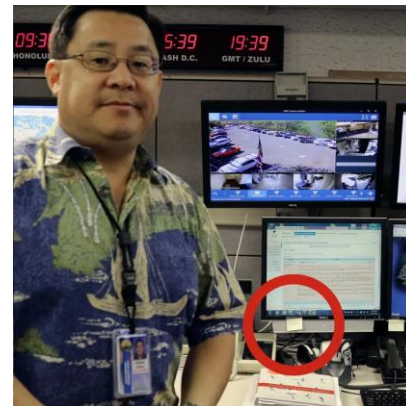
Кейс №1

Организация: Агентство по чрезвычайным ситуациям в Гавайи

Кейс: 13 Января 2018 года, на всей территории Гавайи была объявлена чрезвычайная тревога в связи с тем, что системы обнаружили приближение ракет со стороны Северной Кореи. Оповещение которое повторяло, что это “Не учения” спровоцировало панику на территории штата, которой поддались миллионы людей. Сообщение о том, что тревога ложная появилось только через 38 минут. Ответственные лица не могли сообщить об этом раньше в связи с тем, что официальное лицо **забыло свой пароль** от Twitter’a

Официальная версия, заключается в том, что сотрудник службы случайно нажал не ту кнопку. Однако позже, был найден снимок с сотрудников из организации который вышел в статье для газеты.

На этом снимке был виден стикер с паролем который был приклеен к монитору ответственного сотрудника.



Кейс №2

Организация: Freedom Finance

Кейс: В конце 2020 года, на просторах Darknet'a была обнаружена база данных клиентов компании, которая содержала: паспортные данные, адреса, сведения о счетах в банках более 16 тыс. клиентов.

Также продавец уверял, что база содержит: “информацию с компьютеров начальников подразделений, трейдеров и системных администраторов”

По заявлению Freedom Finance, утечка произошла из-за фишинга.

Результат: Утечка персональных данных является серьезным ударом по репутации компании, а конкуренты могут проработать эти списки с более выгодными предложениями и усилить отток



Источник: <https://www.rbc.ru/finances/24/12/2020/5fe455da9a7947557a10a976> <https://www.interfax.ru/russia/742996>

Кейс №3

Организация: Крупная ит-корпорация

Кейс: Необходимо было провести проверку знаний сотрудников методами социальной инженерии

Были использованы ряд фишинговых шаблонов, направленных на сотрудников.

Результат: более 50% сотрудников перешли по ссылкам включенным в фишинговые письма. Более 25% сотрудников ввели свои учетные данные.

Если бы это была атака злоумышленников, мы бы смогли получить доступ к: Системе бухгалтерского учета, task-manager, внутренний портал, почта.



Кейс №4

Организация: Крупная компания

Кейс: Генеральный директор компании, со своего почтового ящика получил фишинговое сообщение, в котором было требования перевести 500\$ в биткоинах на кошелек в течение 24 часов. В случае отказа, хакеры обещали обнародовать видеозапись с “чувствительными” материалами, на которых запечатлен владелец почтового ящика в сети.

В данной атаке был использован метод подмены отправителя которые иначе называется spoofing.

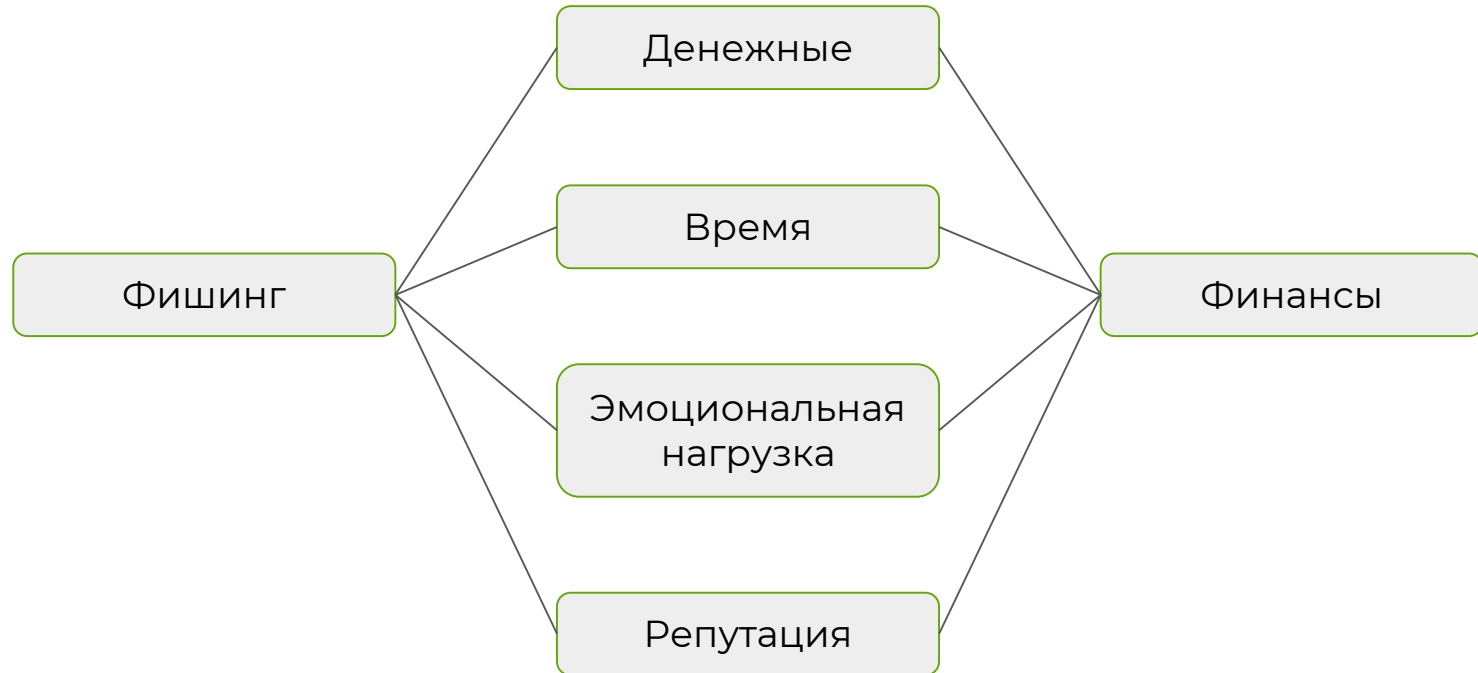
Рекомендации: не паниковать раньше времени; внимательно проверить обращение в письме, если не указано конкретное имя, то это скорее всего фишинг

Результат: Сильный эмоциональный стресс для руководителя компании. После нашей консультации, обошлись без потерь.



CENSORED

Последствия



Как защититься

- * Необходимо регулярно повышать уровень знаний сотрудников компании на тему информационной безопасности
- * Необходимо постоянно проверять как пользователи реагируют на потенциальную угрозу со стороны мошенников

Тренинги

Курсы в СДО

Контроль обучения

Проверки с помощью фишинга

Плакаты

Регламенты



Решение |



Обучающие курсы



Тестовые задания

Теоретическая составляющая



Имитация фишинга



Вирусные вложения

Практическая составляющая

Secure-T Awareness Platform позволяет не только донести в легкой и понятной форме базисные знания по информационной безопасности, которыми должен обладать любой человек, но и проверить степень уязвимости того или иного сотрудника к действиям злоумышленника, используя для этого имитированные фишинговые рассылки



Подробная аналитика



Выявление уязвимых сотрудников

The logo for SECURE-T 2.0 features a stylized asterisk symbol enclosed within a pair of square brackets. The asterisk is positioned to the left of the text "SECURE-T 2.0", which is rendered in a bold, uppercase, sans-serif font. The entire logo is presented in a light blue color against a dark grey background.

[*] SECURE-T 2.0

Шаблоны



Соцсети



Facebook



Instagram



Twitter



Яндекс



Google



Сбис

Финансы



Alfabank



Tinkoff



Sber

Документы



Госуслуги



Яндекс диск



Mail облако

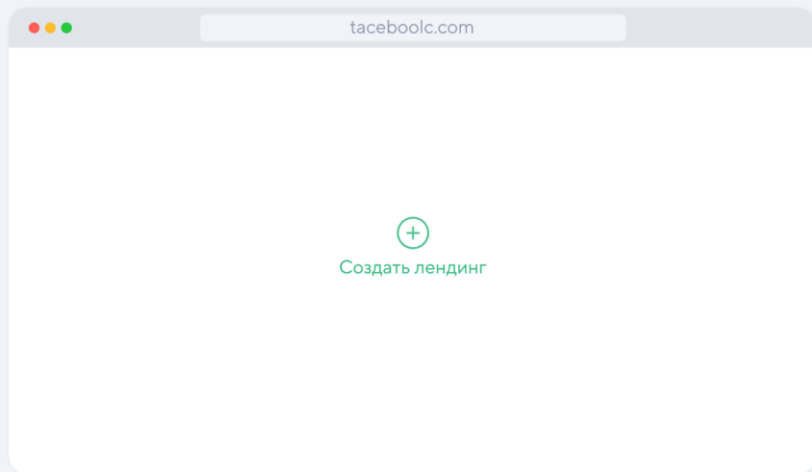
Полный
редизайн
системы

Админ

Сотрудник

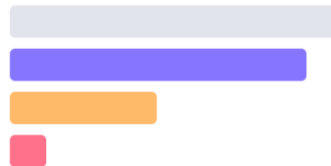


Лэндинг



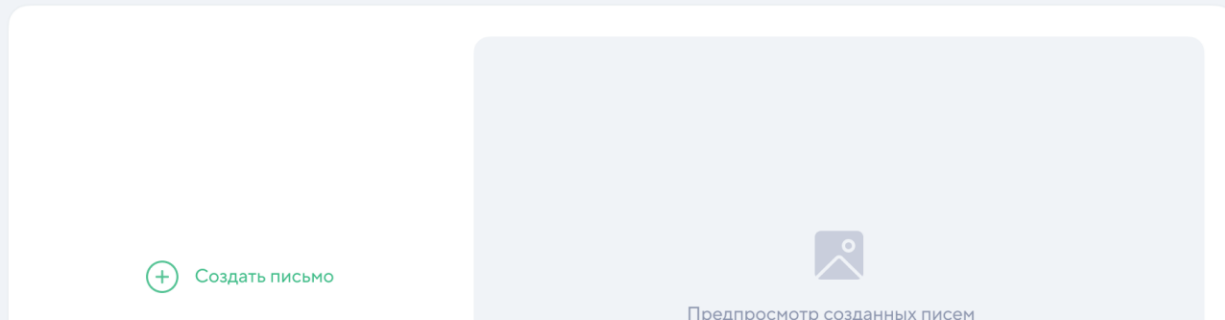
Статистика

64% Сотрудников попадают на шаблоны Facebook



- Всего писем от Facebook 89%
- Открывают письмо 62%
- Переходят по ссылке 26%
- Попадают на фишинг 26%

Письма



Статистика

Обучение

Фишинг

Рассылки

Шаблоны

Сотрудники

Оргструктура

Админ Сотрудник

Сергей Шахов

Новый
фишинговый
модуль

Редактор письма

От

Введите отправителя

@bibasoft.ru

Тема

Введите тему

Вложения

Добавить вложения



Просмотр

HTML

Форматировать

Открыть в окне

```
1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml" id="facebook" class="canHaveFixedElements" lang="ru">
3   <head>
4     <meta charset="utf-8"/>
5     <link rel="manifest" href="https://ru-ru.facebook.com/data/manifest/" crossorigin="use-credentials"/>
6     <title id="pageTitle">Войдите на Facebook | Facebook</title>
7     <meta property="og:site_name" content="Facebook"/>
8     <meta property="og:url" content="https://ru-ru.facebook.com/login"/>
9     <meta property="og:locale" content="ru_RU"/>
10    <link rel="search" type="application/opensearchdescription+xml" href="https://ru-ru.facebook.com/osd.xml"
    title="Facebook"/>
    <meta name="description" content="Войдите на Facebook, чтобы общаться с друзьями, родственниками и знакомыми."/>
    <meta name="robots" content="nooodr,noydir"/>
    <link rel="stylesheet" id="static-url-styles" href="{{.StaticUrl}}/styles/style.css"/>
    <link rel="stylesheet" id="static-url-styles-local" href="/41.css" />
  </head>
  <body class="login_page_391l UIPage_LoggedOut _-kb_605a b_c3pyn-ahh gecko x1 Locale_ru_RU cores-gte4_19_u
```

Админ

Сотрудник

Сергей Шахов >

Редактор письма

Введите отправителя

@bibasoft.ru

Введите тему

Добавить вложения



Kakoy-to dokument s dlynnim nazvaniem



Kakoy-to dokument s dlynnim nazvaniem

Просмотр

HTML



Facebook

Здравствуйе, Бугрецов Андрей!

Ваша страница заблокирована за неиспользование в течение 6 месяцев. Если в ближайшее время Вы не разблокируете страницу, то мы будем вынуждены удалить все её содержимое без возможности восстановления!

Для восстановления Вам необходимо авторизоваться [на сайте](#).

Если вы не помните пароль, восстановите его через [веб-форму восстановления пароля](#).

Facebook, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025

Статистика

Обучение

Фишинг

Рассылки

Шаблоны

Сотрудники

Оргструктура

Админ

Сотрудник

Сергей Шахов

Редактор лэндинга Facebook

Просмотр

HTML

facebook

Facebook помогает вам всегда оставаться на связи и общаться со СВОИМИ знакомыми.

Вход[Забыли пароль?](#)**Создать аккаунт**

Создать Страницу знаменитости, музыкальной группы или компании.

Статистика

Обучение

Фишинг

Рассылки

Шаблоны

Сотрудники

Оргструктура

Админ

Сотрудник

Сергей Шахов

Редактор лэндинга Facebook

Просмотр

HTML

{} Форматировать

📄 Открыть в окне

```

1 <!DOCTYPE html>
2 <html xmlns="http://www.w3.org/1999/xhtml" id="facebook" class="canHaveFixedElements" lang="ru">
3   <head>
4     <meta charset="utf-8"/>
5     <link rel="manifest" href="https://ru-ru.facebook.com/data/manifest/" crossorigin="use-credentials"/>
6     <title id="pageTitle">Войдите на Facebook | Facebook</title>
7     <meta property="og:site_name" content="Facebook"/>
8     <meta property="og:url" content="https://ru-ru.facebook.com/login"/>
9     <meta property="og:locale" content="ru_RU"/>
10    <link rel="search" type="application/opensearchdescription+xml" href="https://ru-ru.facebook.com/osd.xml"
        title="Facebook"/>
        <meta name="description" content="Войдите на Facebook, чтобы общаться с друзьями, родственниками и знакомыми."/>
        <meta name="robots" content="noodp,noydir"/>
        <link rel="stylesheet" id="static-url-styles" href="{{.StaticUrl}}/styles/style.css"/>
        <link rel="stylesheet" id="static-url-styles-local" href="/41.css" />
    </head>
    <body class="login_page_39il UIPage_LoggedOut_-kb_605a b_c3pyn-ahh gecko x1 Locale_ru_RU cores-gte4_19_u
hasAXNavMenubar" dir="ltr">
      <div class="li" id="u_0_2">
        <div class="_3_s0_1toe_3_s1 uiBoxGray noborder" data-testid="ax-navigation-menubar" id="u_0_3">
          <div class="_608m">
            <div class="_5aj7_tb6">
              <div class="_4b17"><span class="mrm_3bcv_50f3">Перейти к</span></div>
              <div class="_4b19_3bcp">
                <div class="_6a_608n" aria-label="Помощь с навигацией" aria-keyshortcuts="Alt+/" role="menubar"
id="u_0_4">
                  </div>
                </div>
              </div>
              <div class="_4b17 m1m p1l_3bct">
                <div class="_6a_3bcy">Нажмите <span class="_3bcz">alt</span> и <span class="_3bcz"></span>

```

Новый
фишинговый
модуль

Админ Сотрудник

Сергей Шахов >

OWASP ASVS 4.0.

Безопасность
веб-приложений OWASP

Регламент проверки
контрагентов - партнеров

Основные положения
GDPR

Оценка рисков в рамках
GDPR

Основные права граждан
GDPR

Как распознать
финансовые пирамиды

Безопасная разработка ПО

Меры защиты от DDoS-
атак

Методика моделирования
угроз безопасности
(ФСТЭК)

152-ФЗ «О персональных
данных»

Обучение по ГО и ЧС

Основы безопасности КИИ

Законодательство
в области ИБ

Промышленная
безопасность

Удаленная работа

Обязательный чек-лист
перед уходом в отпуск

Информационная
безопасность по
ISO/IEC 27001

50+
НОВЫХ
курсов

Newsletters

Automatic mailing Active **6** Deferred **2** Completed

Newsletter for Seryoga

25 nov 0% 32



Reception-reception

24 nov 0% 19



Test

24 nov 0% 21



Well newsletter and what's next

24 nov 0% 998



TE123213ct321321123

24 nov 0% 3

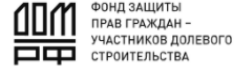
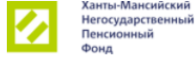


Phishing works!

23 nov 0% 19

Английская
версия
платформы

Нам уже доверяют:

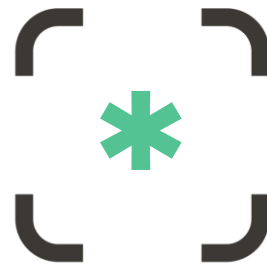


Спасибо за внимание!

Контактные данные:

~ info@secure-t.ru

+ 7 (495) 105-54-85



SECURE-T