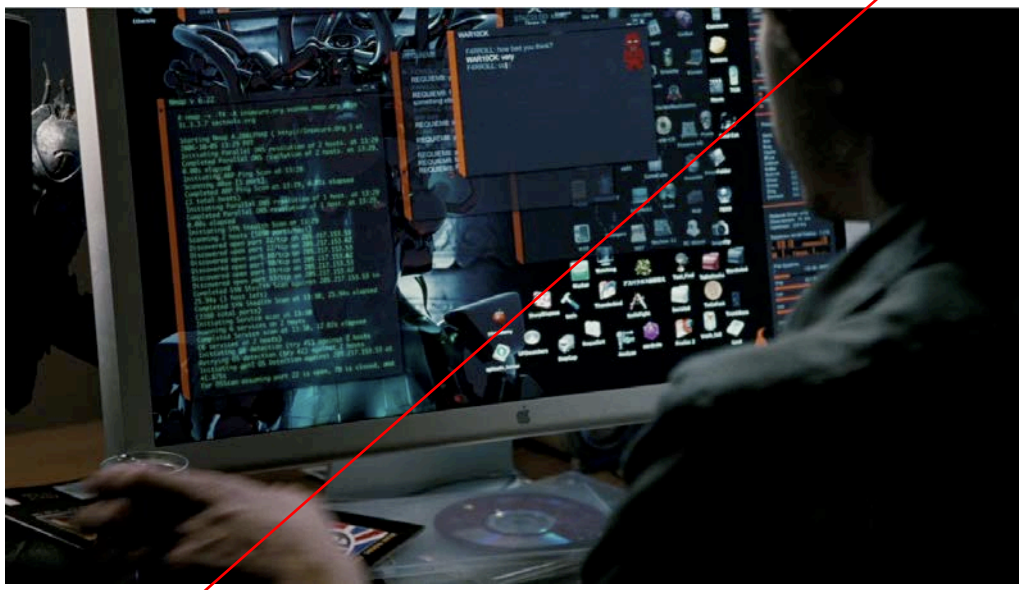
Антифишинг

Статистика для IX Уральского форума –
Информационная безопасность финансовой сферы

февраль 2017

Целевой фишинг: главный вектор атаки



Фишинговые письма – новое цифровое оружие.

Целевой фишинг: главный вектор атаки

ЦБ РФ прогнозирует всплеск атак вредоносных программ в адрес банков к концу 2016 года

«Злоумышленники к концу 2016 года могут активизировать работу по рассылке вредоносных программ в адрес кредитных организаций. После прочтения сотрудниками банков таких посланий происходит заражение программного обеспечения кредитной организации

Артем Сычев, заместитель начальника главного управления безопасности и зашиты информации Банка России – из интервью

Выборка по Антифишинг-проверкам

Дочерняя финансовая компания российского банка

Международный оператор связи (российские филиалы)

Рекламное агентство

Компания-поставщик услуг по безопасности

Аудиторская и консалтинговая компания

Компания-консолидатор по продаже авиационных и железнодорожных билетов

Филиал российского коммерческого банка

Какие сотрудники наиболее уязвимы

Отдел или направление	**Всего проверок**	**Уязвимых сотрудников**
Бухгалтерия	321	55%
Бэкофис	182	50%
ИТ	280	50%
Менеджеры	814	32%

Открыли фишинговые письма, затем перешли по ссылкам или открыли вложенные файлы

В филиале банка

Отдел или направление	**Проверено сотрудников**	**Уязвимых сотрудников**
Менеджеры	48	35%
Бэкофис	42	17%
ИТ + ИБ	11	19%

Открыли фишинговые письма, затем перешли по ссылкам или открыли вложенные файлы

Классификация проверочных фишинговых атак

Анонимное - без указания ФИО сотрудника
Персональное - с указанием ФИО

Внешнее – от имени внешних партнеров или подрядчиков
Корпоративное – письмо из своей организации
Личное – личное письмо сотруднику

Пример – корпоративное письмо

Сб 19.03.2016 22:04

Отдел поддержки пользователей

Новый стандарт подписи

Кому Sergey

Коллеги, добрый день!

Уведомляем вас, что с 19.03.2016 вводится новый корпоративный стандарт подписи для электронной почты.

Вам необходимо самостоятельно изменить стандартный шаблон подписи.

Со следующей недели использование старых подписей не допускается.

По ссылкам вы найдете новые шаблоны и инструкцию по изменению.

Отдел поддержки пользователей и ИС
Управление по информационным технологиям

phone: +7 495 0
rus.support@

Анонимное Корпоративное

Пример – внешнее письмо от партнеров

Компрометация АРМ КБР

info@fincert.net <info-fincert@ ru>
кому: мне

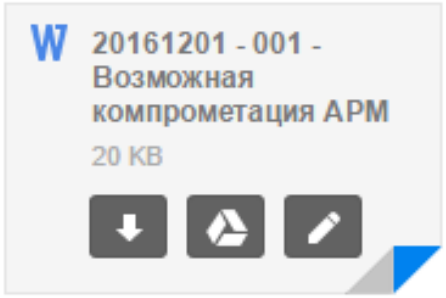
Здравствуйт! Отправляем важную информацию касательно компрометации банковских систем.

-

С уважением,

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

тел. +7 (499) 772-70-90



Анонимное Внешнее

Самые эффективные проверки

Тип письма	**Отправлено писем**	**Эффективность**
Анонимное корпоративное	678	46%
Персональное личное	307	44%
Персональное корпоративное	304	38%
Анонимное внешнее	708	37%

Эффективность = процент сотрудников, которые открыли фишинговые письма, затем перешли по ссылкам или открыли вложенные файлы

Дополнительная статистика

12 с минимальное время от начала проверки до взлома первой жертвы

- Google Chrome версий от 4.0 до 49.0
- Mozilla Firefox версий от 19.0 до 45.0
- Opera 12.16
- Microsoft IE версий 7-10
- Microsoft Windows XP

Устаревшие версии IOS, Android, MacOS

Во всех проверках на рабочих местах сотрудников находились устаревшие приложения или операционные системы с уязвимостями