Обеспечение бесперебойной работы казначейства

Фишман Антон

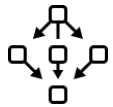
Руководитель департамента системных решений

Ландшафт угроз – COVID-19

Целевые атаки

Рост количества целевых атак на сотрудников банков

Инсайдеры



Рост числа инсайдерских атак с использованием тех категорий сотрудников, которым снижают з/п или сокращают при переходе на удаленный режим работы.

Социальная инженерия

Увеличение мошеннической активности по отношению к людям пожилого возраста: доставка товаров на дом, предложения лекарств и тестов на COVID-19

Вредоносные рассылки

Рост числа вредоносных рассылок для заражения пользователей вирусами-шифровальщиками, банковскими троянами, программами-шпионами

Шпионаж

Повышение риска проведения атак с целью шпионажа

Мошенничество

Мошеннические бесплатные сервисы: платформы для проведения видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, фейковых мобильных приложений для доставки еды

Угрозы для юридических лиц

Недостаточное внимание безопасности при организации удаленной работы

Отсутствие тестирования реализованных систем

Люди, работающие из дома, меньше заботятся о своей безопасности, нежели на работе

Необходимость организации бизнес-критичных процессов удаленно

APT и злоумышленникам гораздо проще атаковать чем раньше, появились новые уязвимости

Злоумышленники переключились с крупных компаний на SMB

Инсайдеры – уволенные сотрудники, имеющие доступ к внутренней информации

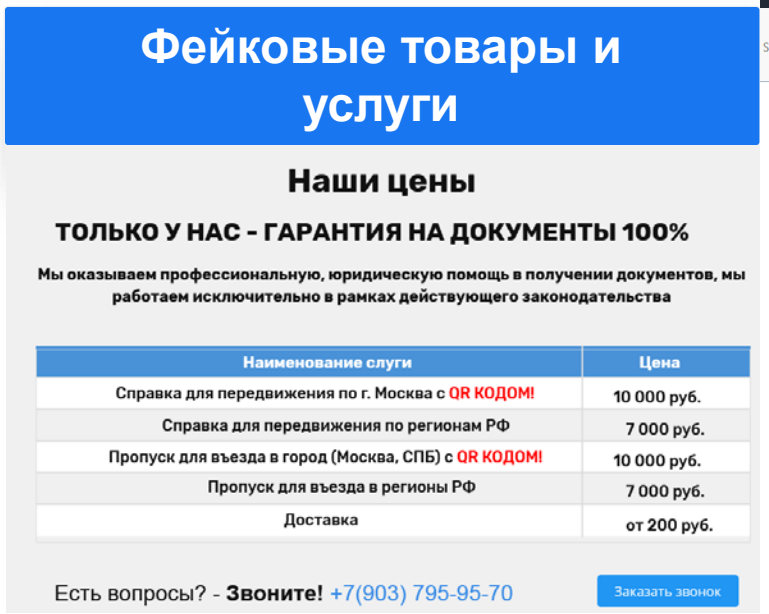
Отсутствие систем защиты от современных атак

Недостаточный уровень киберграмотности

Атака всегда начинается с человека

90% успешных атак – с фишинга, звонка

Фейковые товары и услуги



Наши цены

ТОЛЬКО У НАС - ГАРАНТИЯ НА ДОКУМЕНТЫ 100%

Мы оказываем профессиональную, юридическую помощь в получении документов, мы работаем исключительно в рамках действующего законодательства

Наименование слуги	Цена
Справка для передвижения по г. Москва с QR КОДОМ!	10 000 руб.
Справка для передвижения по регионам РФ	7 000 руб.
Пропуск для въезда в город (Москва, СПБ) с QR КОДОМ!	10 000 руб.
Пропуск для въезда в регионы РФ	7 000 руб.
Доставка	от 200 руб.

Есть вопросы? - **Звоните!** +7(903) 795-95-70 Заказать звонок

Вредоносное ПО

From Dr. Stella Chungong <rasheed@wakeikai.com>
Subject SAFETY COVID-19 (Coronavirus Virus) AWARENESS
To Recipients <rasheed@wakeikai.com>
Reply Reply All Forward More
23.03.2020, 2:28

World Health Organization

To whom it may concern,

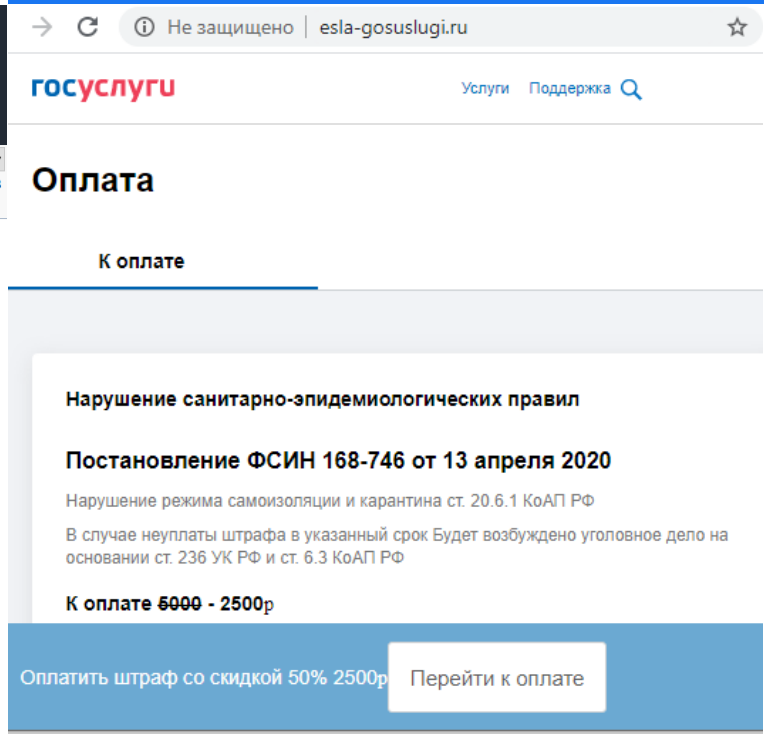
Go through the attached document on safety measures regarding the spreading of Corona-virus.

Common symptoms include fever, cough, shortness in breath and breathing difficulties.

Regards.

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Фишинг



Не защищено | esla-gosuslugi.ru

госуслуги Услуги Поддержка

Оплата

К оплате

Нарушение санитарно-эпидемиологических правил

Постановление ФСИН 168-746 от 13 апреля 2020

Нарушение режима самоизоляции и карантина ст. 20.6.1 КоАП РФ

В случае неуплаты штрафа в указанный срок Будет возбуждено уголовное дело на основании ст. 236 УК РФ и ст. 6.3 КоАП РФ

К оплате ~~5000~~ - 2500р

Оплатить штраф со скидкой 50% 2500р Перейти к оплате

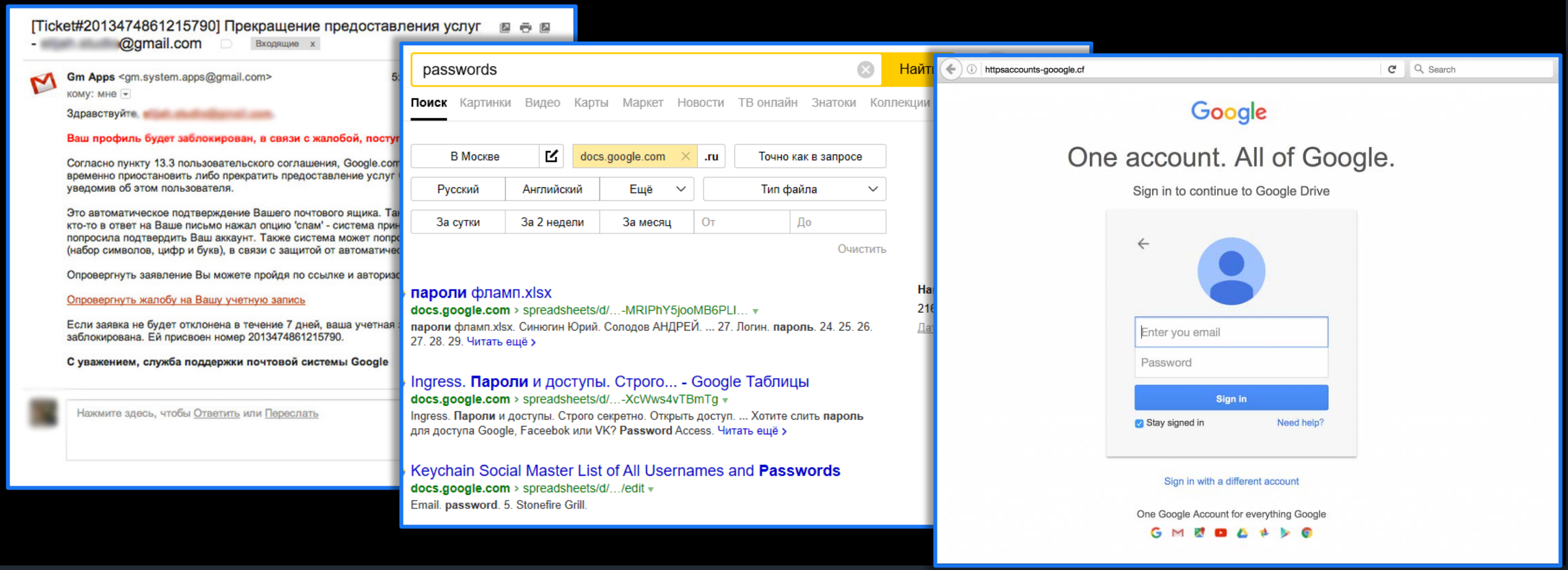
Вечные правила цифровой гигиены

GROUP-IB

Помните про фишинговые рассылки

Используйте разные и сложные пароли

Будьте бдительны про работе с подозрительными сайтами



Рекомендации для юридических лиц и казначейства

1) Проведите обучение для пользователей.

2) Проверьте, настроена ли двухфакторная аутентификация в почте, в мессенджерах и при VPN подключении

3) Обязательно проверьте свою домашнюю сеть
- смените пароль на WIFI сети,
- убедитесь что используется WPA-2 ,
- смените пароль на роутере,
- обновите прошивку на роутере,
- обновите прошивку и смените пароли на всех ваших домашних IoT устройствах.

4) Обновите операционную систему на домашнем ПК, и установите на него систему защиты для рабочих станций

3) Заранее позаботьтесь о получении удаленного доступа к необходимым ресурсам и следуйте указаниям IT-специалистов для его настройки.

4) По возможности работайте на корпоративном компьютере. Не загружайте и не открывайте корпоративные файлы на личных устройствах.

5) Организуйте внешний аудит для компании, чтобы убедиться, что IT/ИБ специалисты подготовились к безопасной удаленной работе.

6) Будьте бдительны - Домашняя сеть не защищается отделом ИБ, поэтому будьте внимательны — атакующие могут воспользоваться ситуацией.

Рекомендации для юридических лиц и казначейства

При работе с банк-клиентом

- Желательно использовать многофакторную аутентификацию, где помимо аппаратного ключа, используется еще и одноразовый пароль/SMS
- Используйте банк-клиент ТОЛЬКО на специально выделенном компьютере, на котором желательно ничего больше не делать, а еще лучше – использовать для этой цели виртуальную машину, к которой вы подключаетесь через VPN с 2=х факторкой.
- При использовании WEB-клиента, лишний раз убедитесь, что адрес сайта верный, а также что браузер не ругается на сертификат – что сертификат действительно выдан на имя Вашего банка.
- Также обязательно используйте 2-ой фактор, как для подтверждения входа в систему, также и для подписи с помощью аппаратного ключа.

Предотвращаем и расследуем киберпреступления с 2003 года

Фишман Антон

Руководитель департамента системных решений

www.group-ib.ru
info@group-ib.com
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+7 495 984 33 64
facebook.com/groupib
instagram.com/group_ib