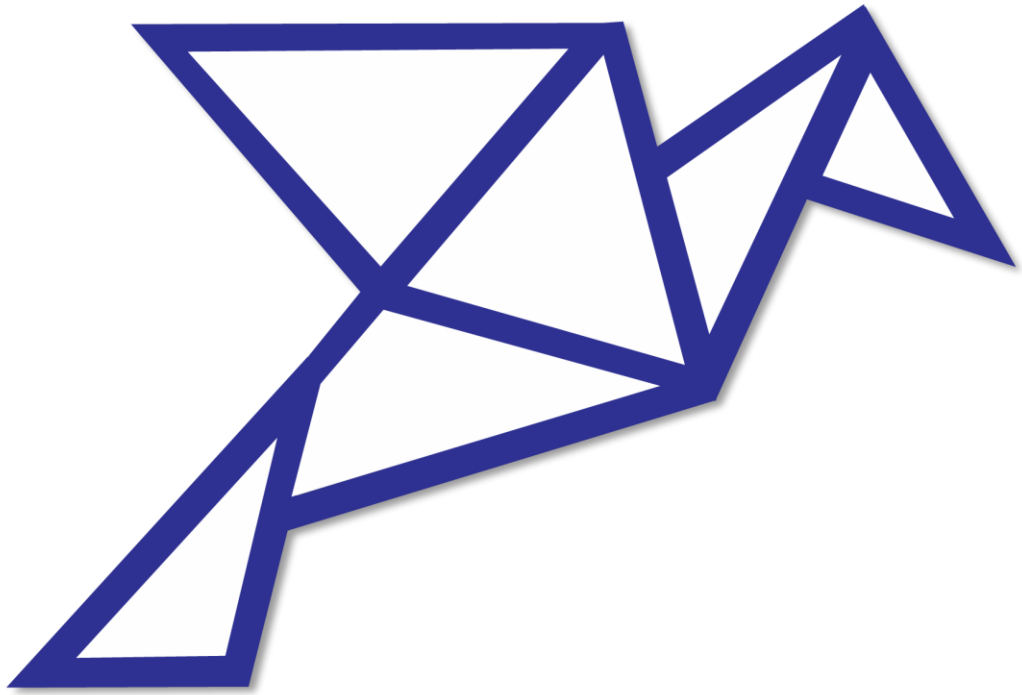
Правила цифровой гигиены

или как не попасть на крючок злоумышленника



Игорь САВИН
Менеджер проектов

PACIFICA

#SID2019 #SaferInternetDay #Pacifica

Safer Internet Day 2019 | Tuesday 5 February

Together for a better internet

www.saferinternetday.org

European Commission

INHOPE

ins@fe

О компании

PACIFICA

10 лет на рынке ИБ Казахстана

10 ЛЕТ

На рынке информационной безопасности Казахстана

Резиденты - 100%

ПЕРВАЯ в Казахстане

Компания, которая занимается только проектами в области обеспечения информационной безопасности

intella

БИЗНЕС БЕЗОПАСНОСТИ

Более 20 мировых вендоров

Лицензия КНБ РК СК №013
на занятие разработкой и реализацией (в том числе иной передачей) средств криптографической защиты информации

- **Алматы** – Центральный офис
- **Астана** – Дополнительный офис

bsi.
ASSOCIATE CONSULTANT PROGRAMME
MEMBERSHIP NUMBER 726

Программа ассоциированных консультантов (ACP), созданная мировым лидером в разработке методологии построения систем управления – компанией BSI, объединяет профессионалов в сфере разработки и сертификации систем менеджмента.

Собственный ЦЕНТР по расследованию инцидентов

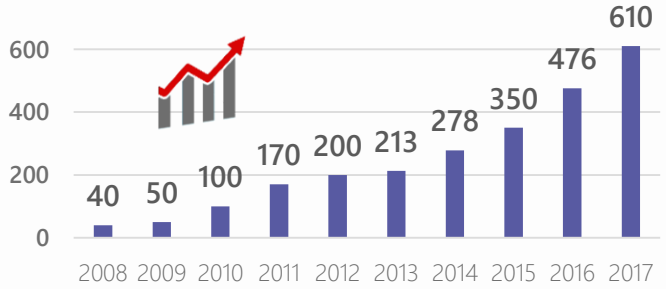
SERT

25

сотрудников

Собственный учебный центр «INTELLA»

Оборот (млн. тг.)



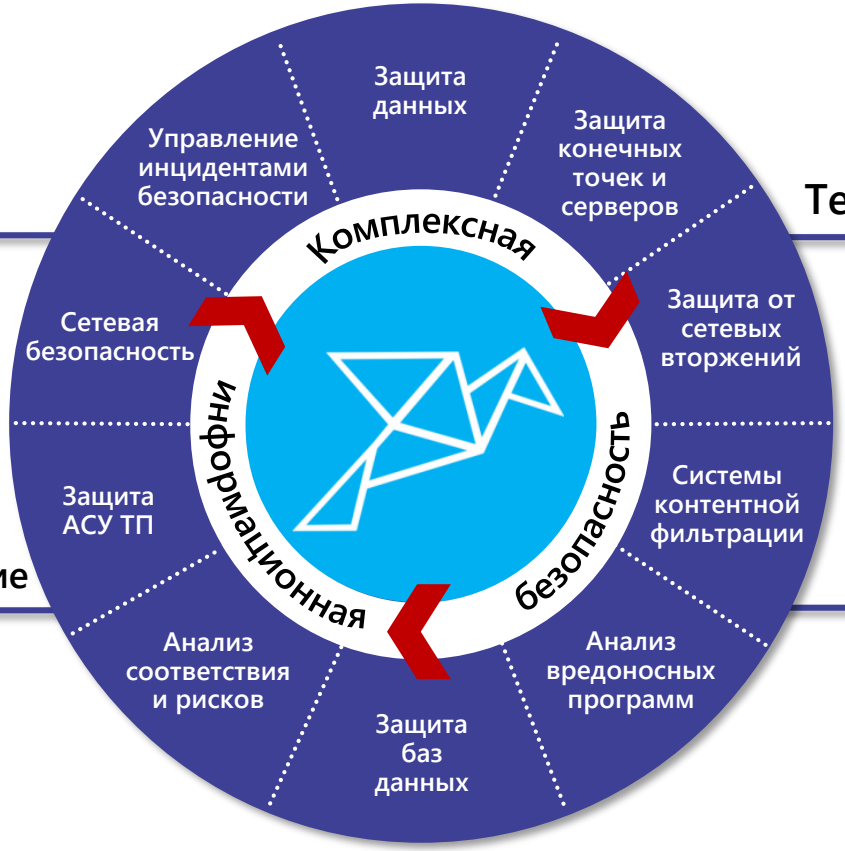
Направления деятельности

Аудит и консалтинг

- Подготовка к аудиту в соответствии с международными стандартами (ISO 27001, PA/PCI DSS)
- Консультации по вопросам обеспечения информационной безопасности

Проектирование и внедрение

- Проектирование и внедрение систем информационной безопасности
- Построение центра управления инцидентами, защита центров обработки данных (ЦОД)



Техподдержка и аутсорсинг

- Поддержка и сопровождение систем информационной безопасности (СИБ)
- Оптимизация ИБ-инфраструктуры, ИБ-аутсорсинг, облачные ИБ-сервисы

Обучение

- Проведение тренингов и обучающих семинаров менеджеров и технических специалистов ИБ
- Обучение специалистов ИБ по собственным программам

ТОО «ПАЦИФИКА» предоставляет комплекс решений и услуг, позволяющих нашим клиентам выстраивать систему обеспечения информационной безопасности «с нуля» или оптимизировать существующую

Безопасность в сети Интернет

PACIFICA

Правила безопасности нужны, чтобы защитить информационные активы

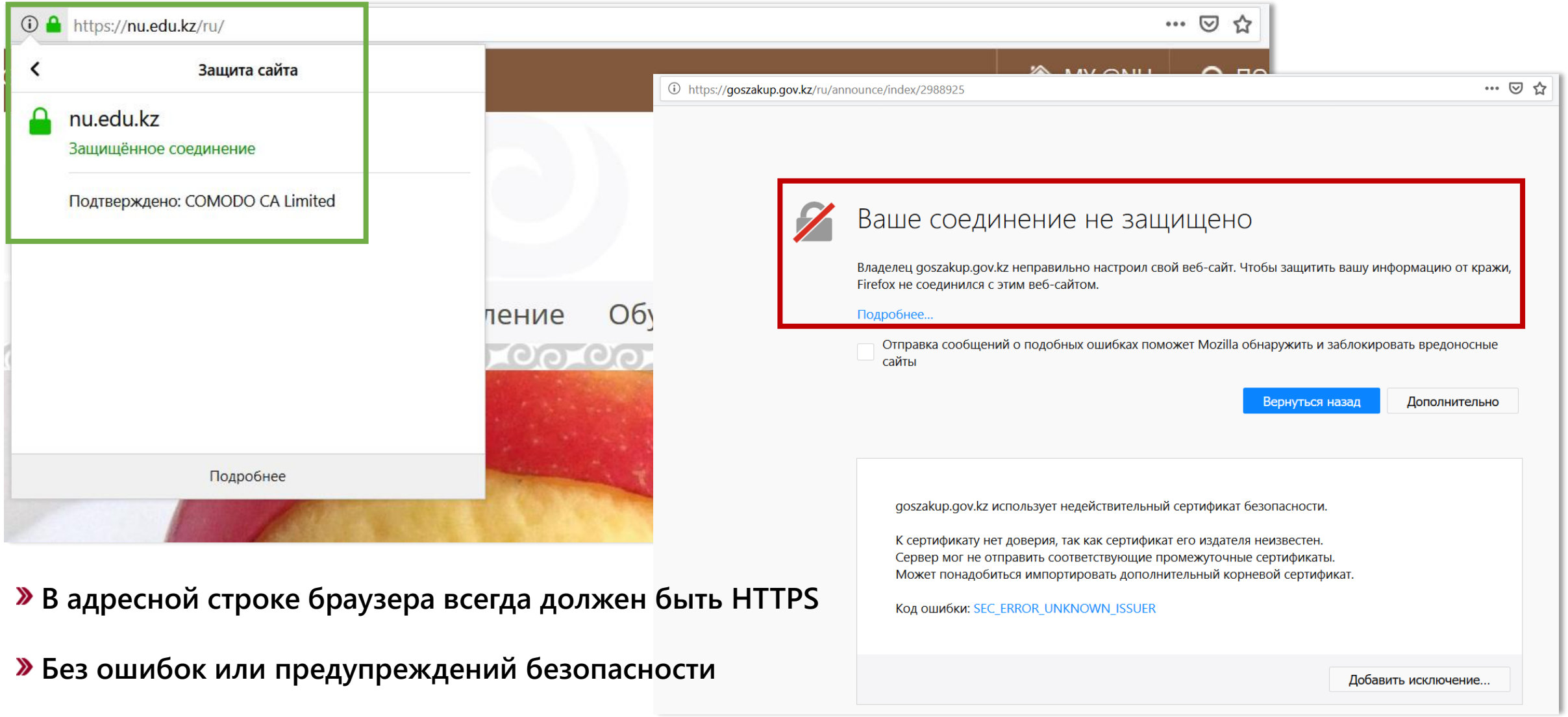
К информационным активам относятся:

- Персональные данные
- Информация, в том числе конфиденциальная
- Компьютерные системы
- Люди

Злоумышленники чаще всего используют сайты и электронную почту, чтобы взломать нас и/или нашу компанию

```
Mixed Content: The page at                                    simple-example.html:1
'https://googlesamples.github.io/web-fundamentals/samples/discovery-and-
distribution/avoid-mixed-content/simple-example.html' was loaded over HTTPS, but
requested an insecure script 'http://googlesamples.github.io/web-
fundamentals/samples/discovery-and-distribution/avoid-mixed-content/simple-
example.js'. This request has been blocked; the content must be served over HTTPS.
```

Безопасность при работе с сайтами

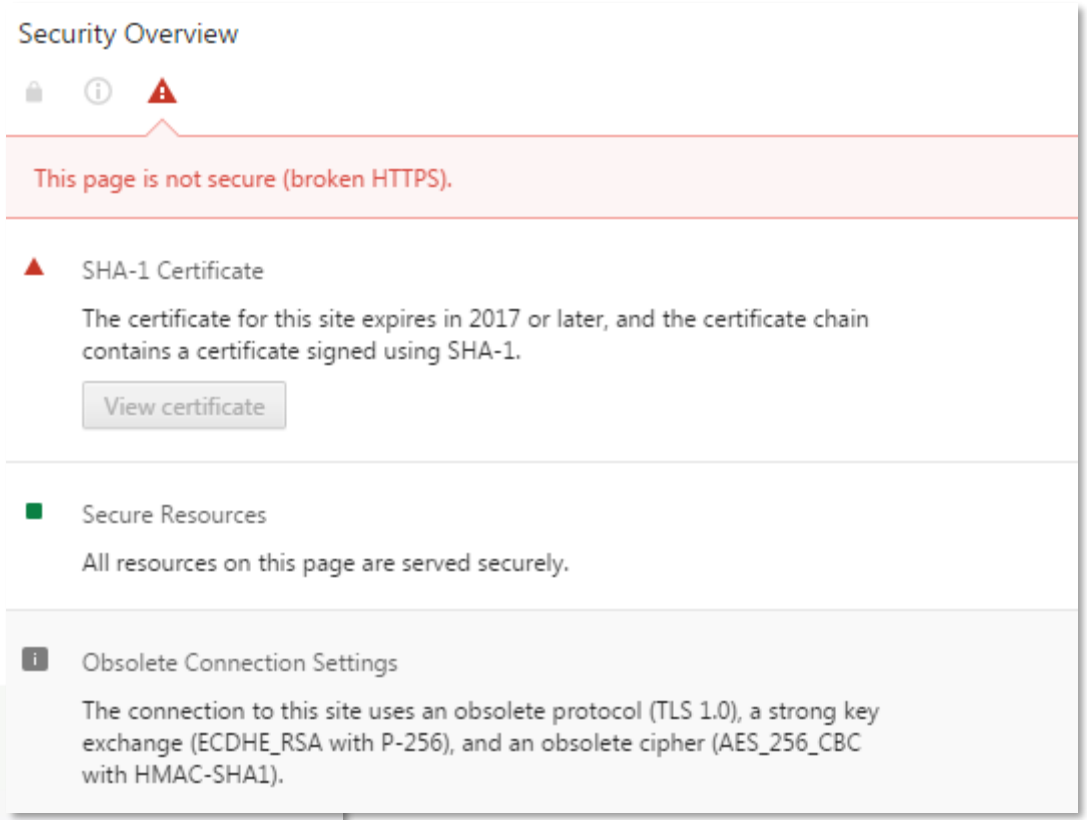


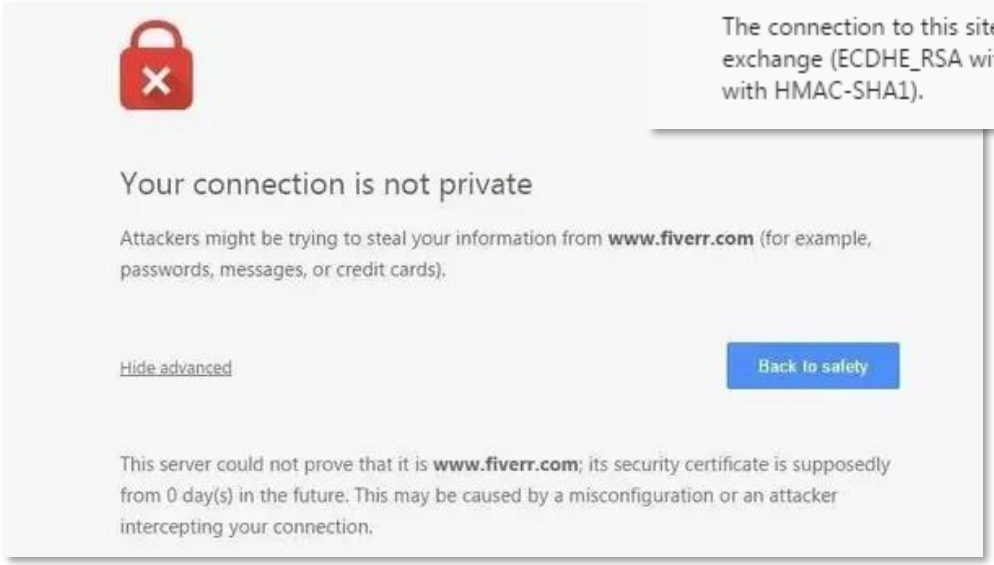
- В адресной строке браузера всегда должен быть HTTPS
- Без ошибок или предупреждений безопасности

Интернет-сайты с ошибками

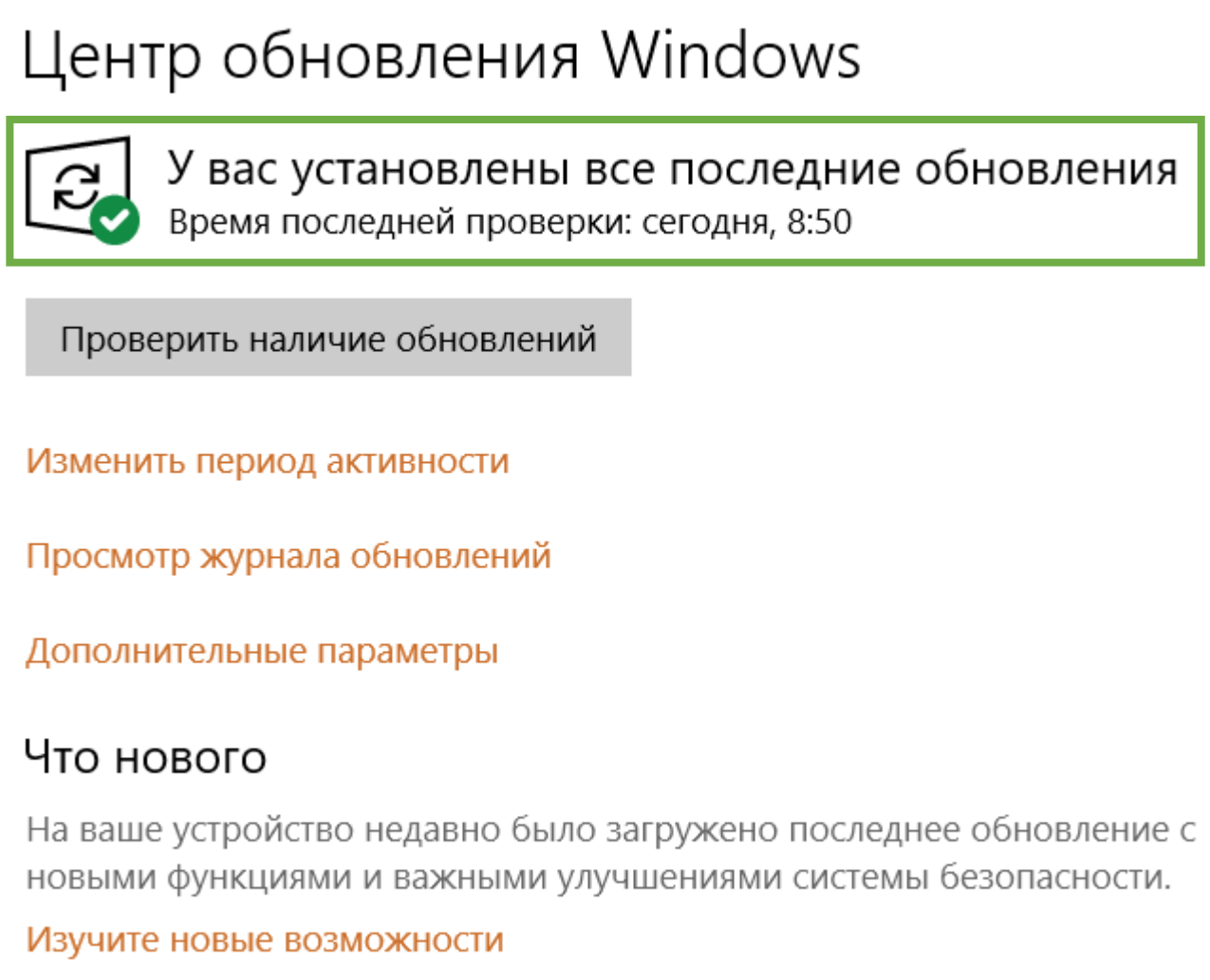
Если вы увидели ошибку HTTPS:

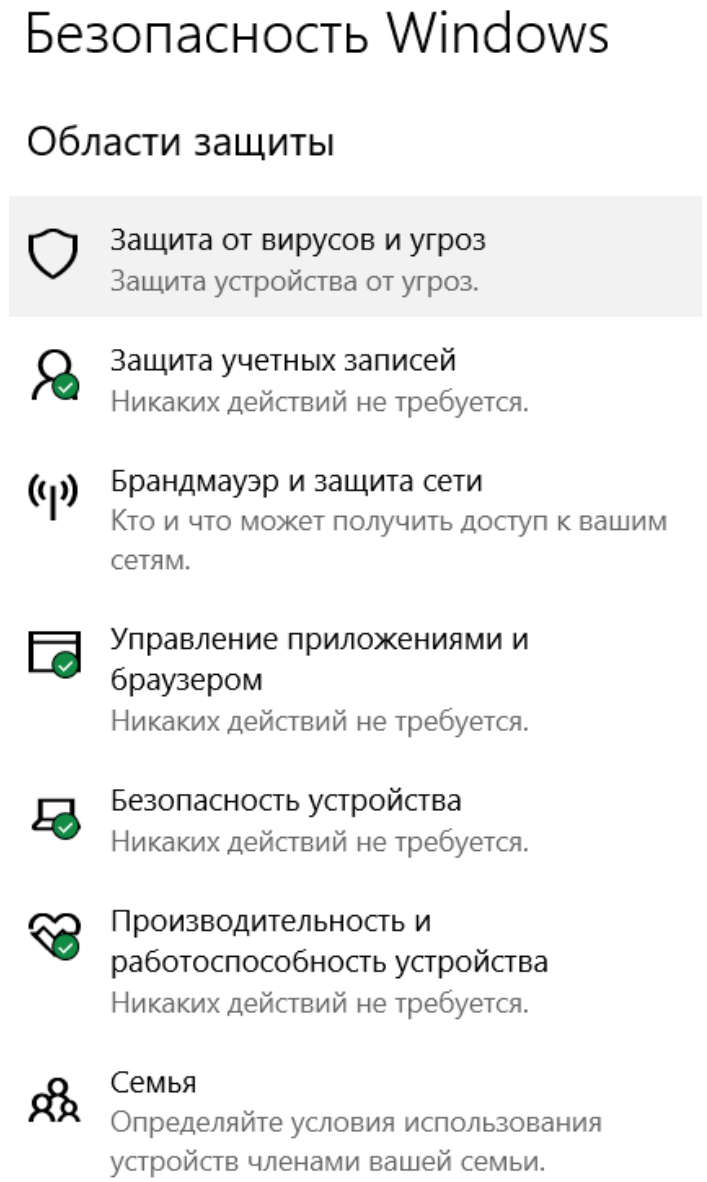
- Не вводите свои логин и пароль на таком сайте
- Если вы подключены не к корпоративному/доверенному Wi-Fi:
  - Подключитесь через мобильную сеть и проверьте, исчезла ли ошибка
  - Если ошибка исчезла, возможно вы стали жертвой атаки злоумышленников в сети, к которой были подключены





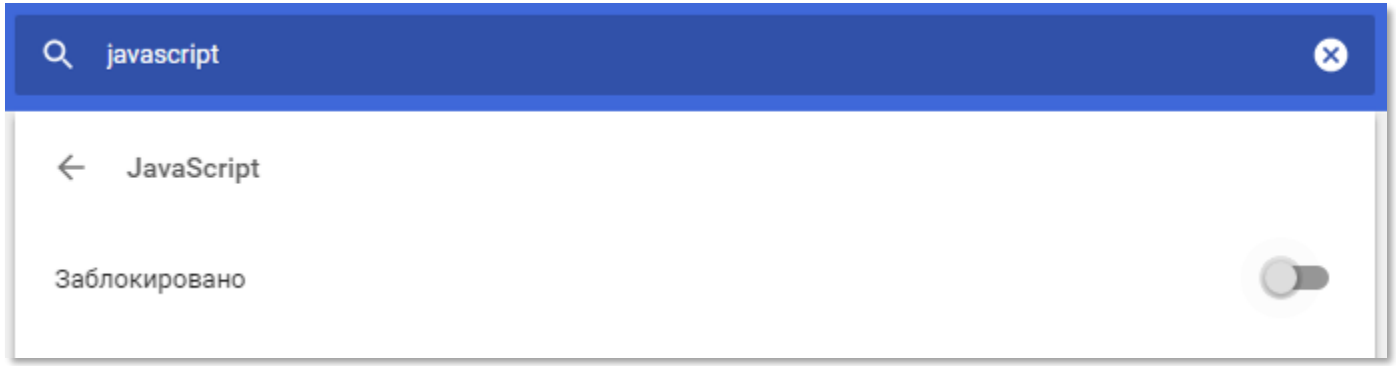
Обновляйте свою систему и все программы

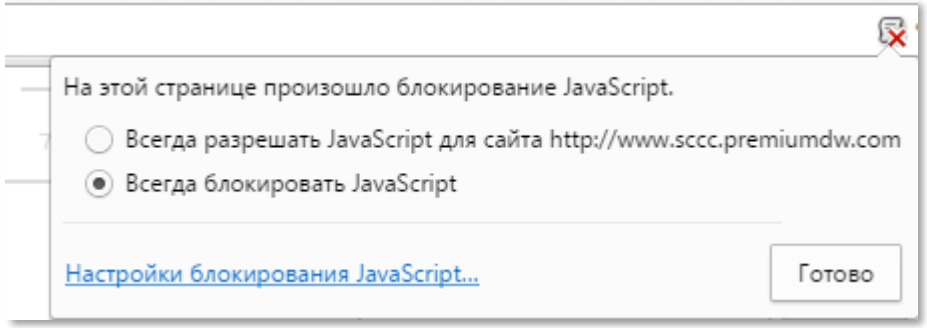




Защитите свой браузер

- Заблокируйте и включайте JavaScript только на известных сайтах
- Отключите выполнение скриптов и все лишние плагины
- Удалите JAVA

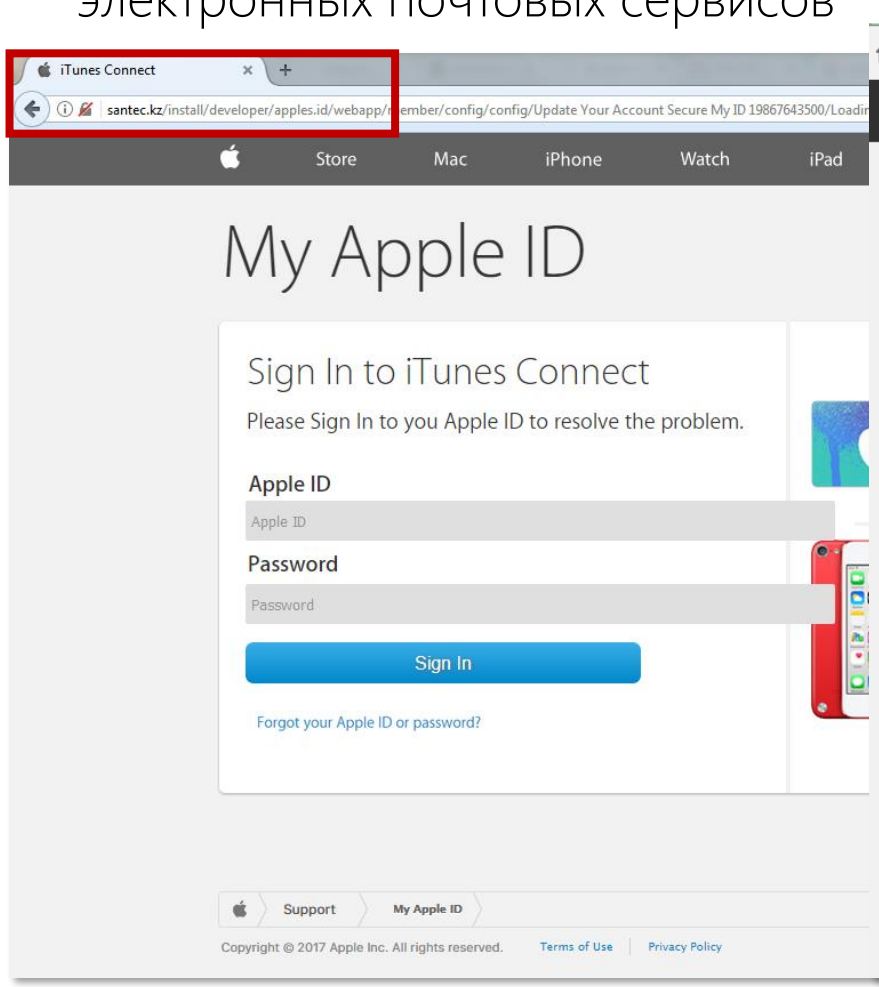


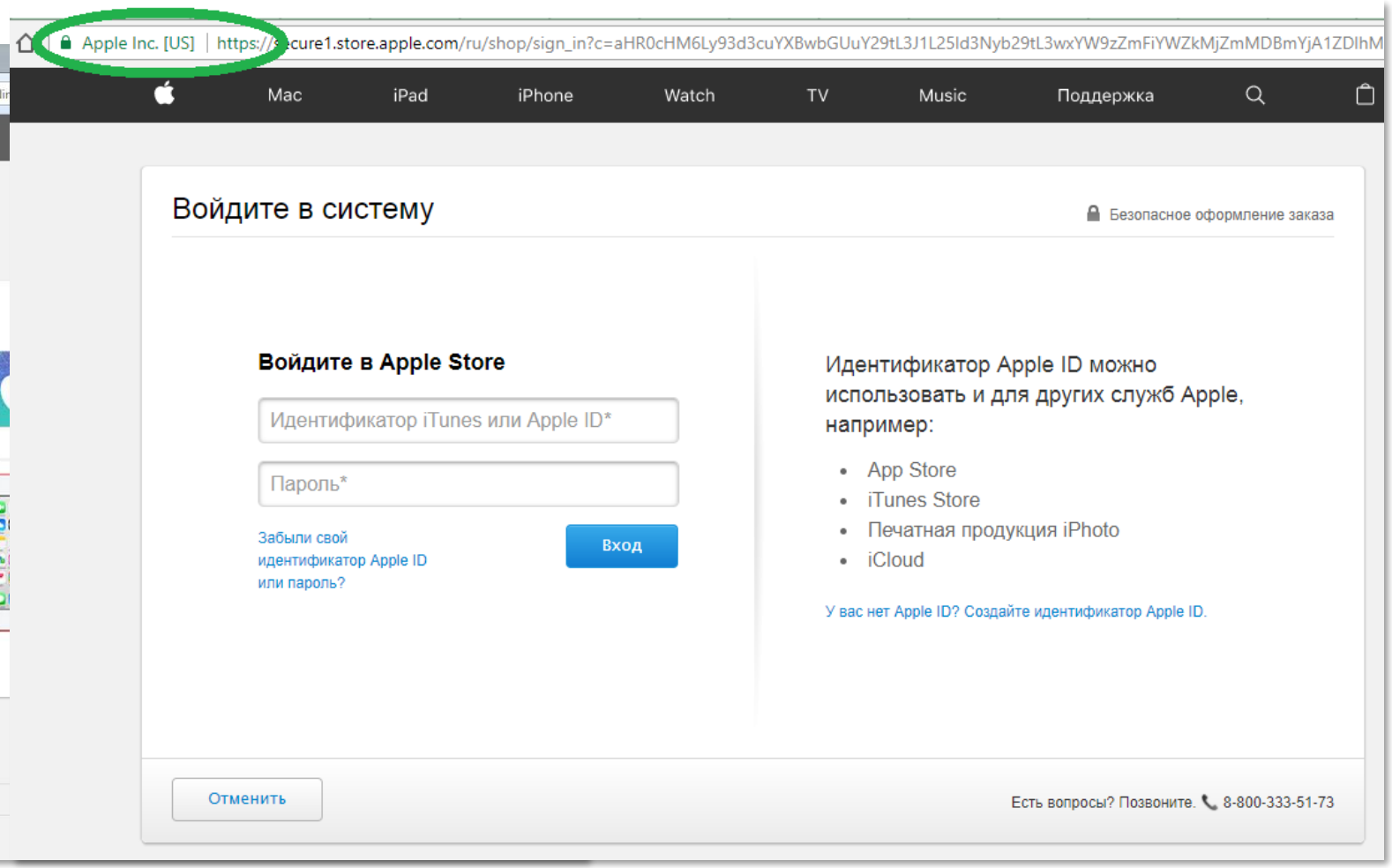


Данные действия защитят ваш браузер от большинства атак со стороны зараженных сайтов

Будьте очень внимательны, по каким ссылкам вы переходите

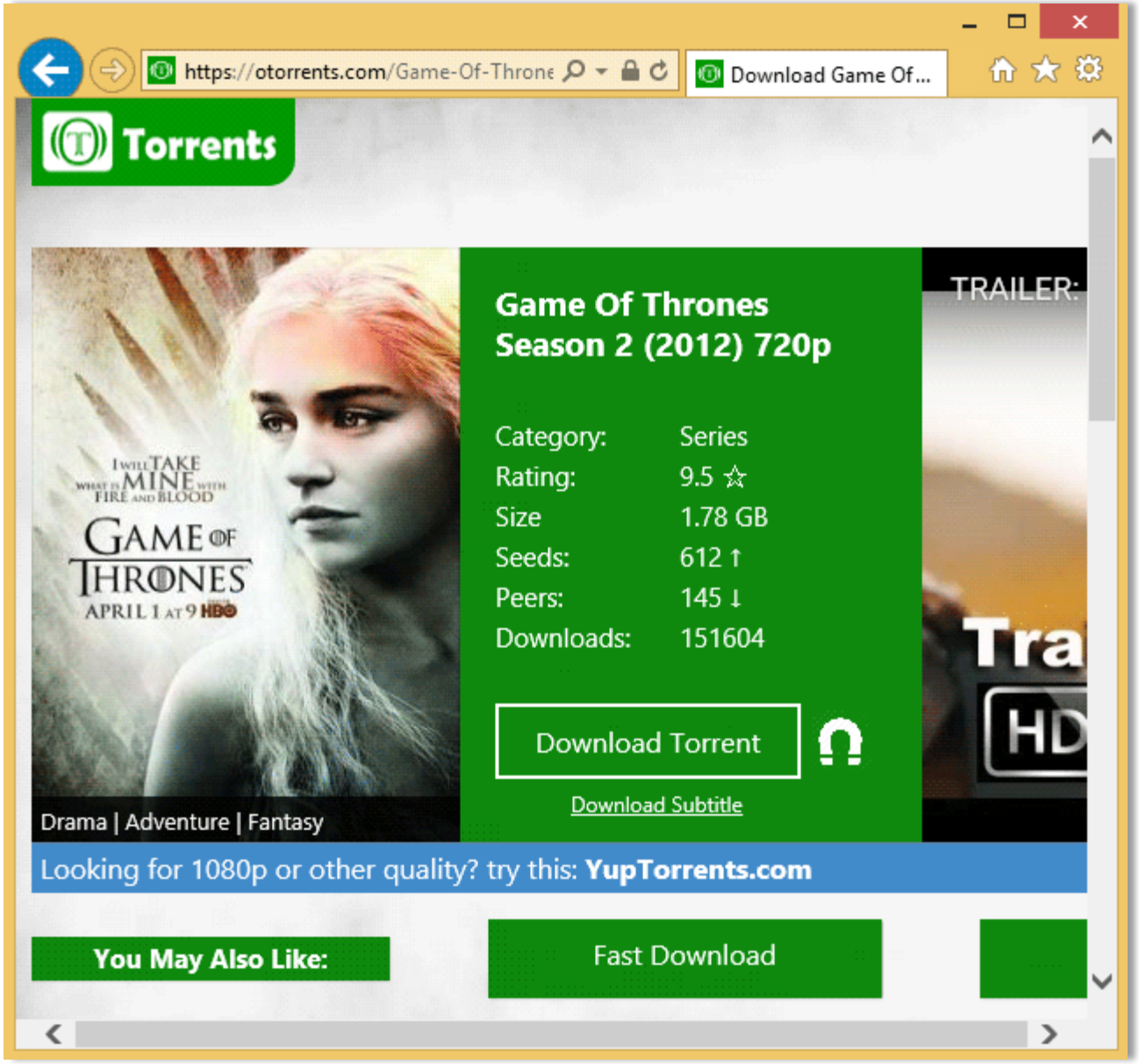
- Есть сайты, которые маскируются под официальные страницы платежных систем и электронных почтовых сервисов





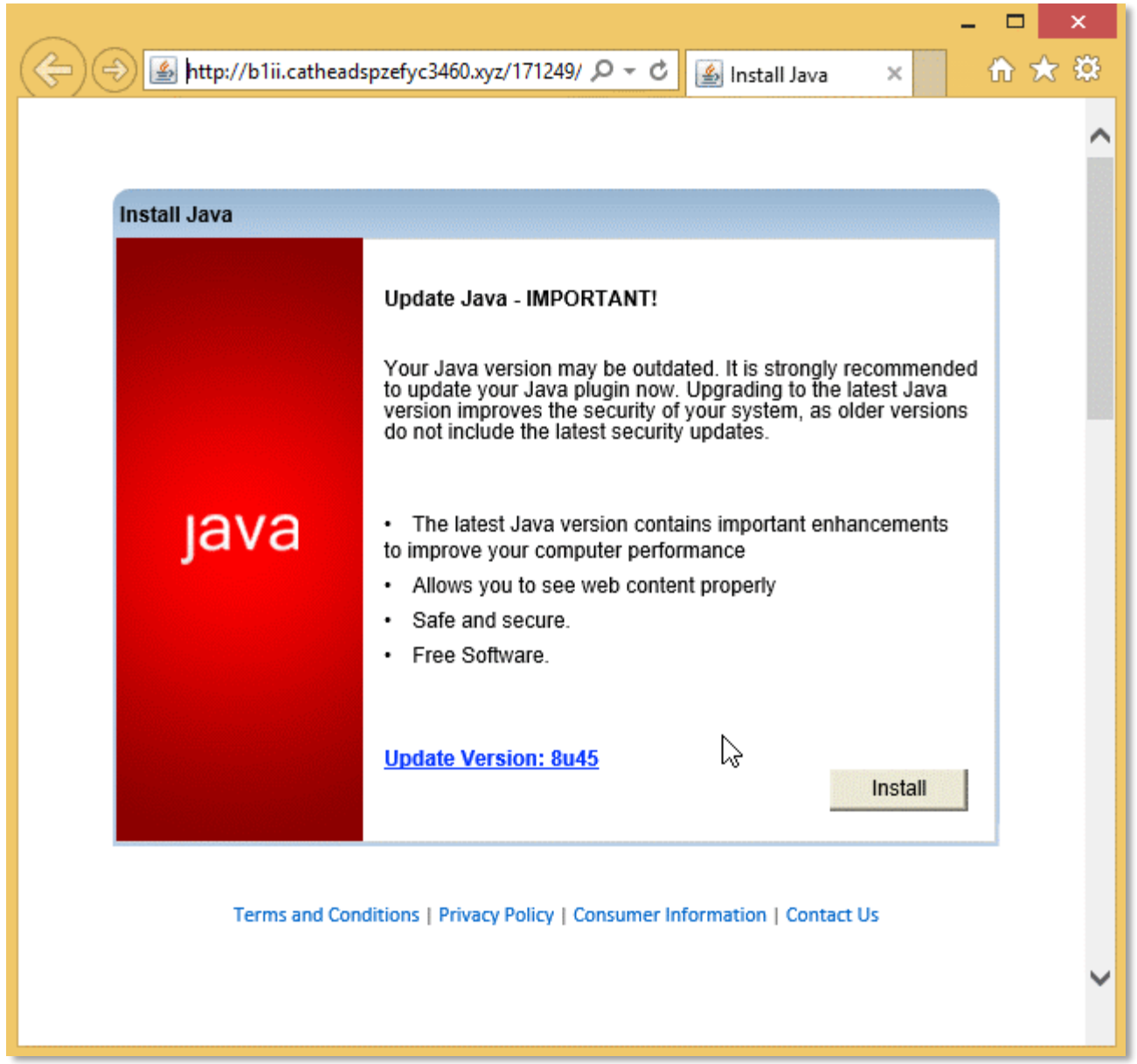
Не заходите на подозрительные сайты

- Злоумышленники заманивают вас на сайт, на котором предлагают скачать что-то полезное



Не скачивайте неизвестные файлы

- Сайт сообщает о важном обновлении или какой-то проблеме, которую необходимо решить. Для этого вам предлагают скачать файл или установить программу



Не запускайте скачанные программы

- После запуска такая программа поможет взломать ваш компьютер, предоставив злоумышленнику удаленный доступ к конфиденциальной информации, или зашифрует все файлы и потребует выкуп

Безопасность при работе с почтой

PACIFICA

Терминология

- **Спам** – навязчивая электронная рассылка, почтовый мусор, незапрошенная пользователем информация

Основное свойство: анонимность. Все страдают, в основном, именно от автоматических рассылок со скрытым или фальсифицированным обратным адресом

- **Фишинг** – (англ. phishing, от *fishing* - рыбная ловля, выуживание и *password* - пароль) – вид интернет-мошенничества, цель которого получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации

Почта и фишинг

Целевой фишинг – отправка специального вредоносного письма. Это самый простой и популярный способ взломать вашу компанию

Бұл автоматты түрде жасалатын электрондық пошта, Өтінеміз, ЖОҚПАҢЫЗ. Кез келген жауап электрондық пошта назардан тыс қалады.

Қауіпсіздік кеңестері

1. Компьютерде вирусқа қарсы бағдарламалық құралды және жеке брандмауэр орнатыңыз. Сізге соңғы қорғауды
2. Вирустар мен басқа да жағымсыз мәселелерді болдырмау үшін белгісіз немесе сенімді емес көздерден тіркемел
3. Егер сіз кез-келген ерекше әрекетті тапсаңыз, мүмкіндігінше тез арада осы төлемнің жіберушісіне хабарласыңы

kaspi bank

Төлемді растау

HS

Halyk Savings Bank of Kazakhstan JSC <fghyun@hanmail.net>
afk@afk.kz
понедельник, 19 ноября 2018 г., 15:38
Показать сведения

Төлемді растау.iso
2,4 МБ

Скачать все Просмотреть все

HALYK BANK

Қосылған төлем кеңесі біздің тапсырыс берушінің талабы бойынша беріледі. Кеңес тек анықтама үшін.

Кеңес Ref: [G60401849228]

Тапсырыс беруші: [2000003926SG0017]

Төлем бөлшектері: SEE ATTACHED
Сома: 57,087.09
Валюта: EUR

Сізге шын берілген,

Как работает фишинговая атака

1. Потенциальная «жертва» получает фишинговое письмо
2. «Жертва» переходит по ссылке в письме или открывает вложенный в письмо файл
3. Злоумышленник получает контроль над компьютером «жертвы»
4. Злоумышленник проникает в сеть, крадет пароли, номера кредитных карт, банковских счетов и другую конфиденциальную информацию или шифрует данные, начиная шантажировать «жертву»

90%

всех целевых атак
начинается с фишинга

Как понять, что вам пишут или звонят злоумышленники

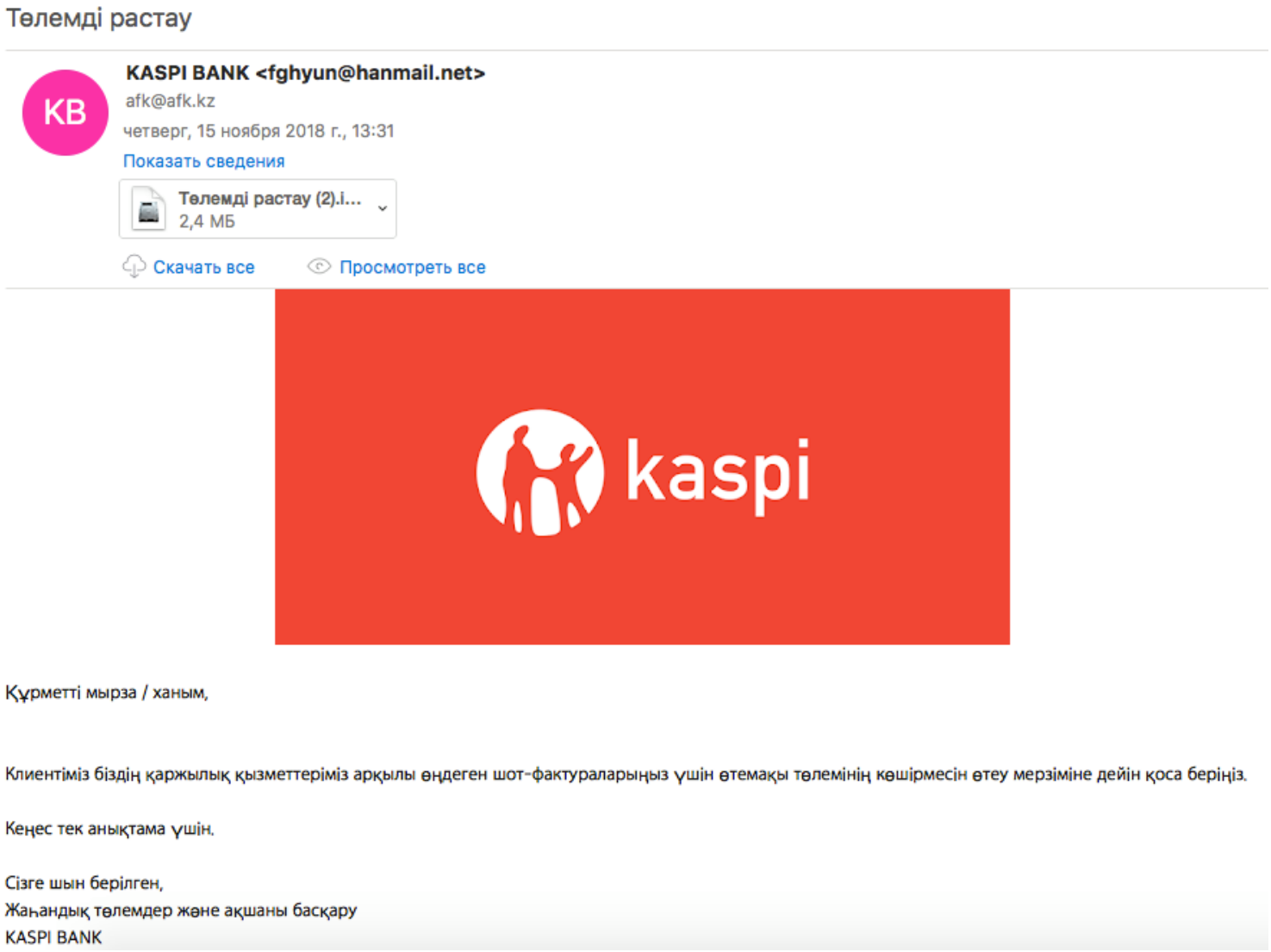
- Стараются использовать ваши слабости, чтобы достичь своих целей – получить информацию или побудить вас сделать что-то
- Слабости вызывают сильные эмоции и позволяют на секунду отключить критическое мышление
- Секунды вполне хватит, чтобы кликнуть по ссылке или открыть вложенный файл

Слабости, которые используют злоумышленники:

- Страх: «Ваш компьютер заражен и заблокирован. Кликните здесь»
- Невнимательность: «www.sbernbank.kz», «www.gmall.com»
- Жадность: «Скидка 50% при оплате прямо сейчас»
- Раздражение: «Чтобы отписаться, перейдите по ссылке»
- Желание помочь: «Ваш коллега потерял вещи, дайте мне его номер»
- Любопытство: «Смотри, как ты отжигаешь на этом видео»
- Авторитет/Срочность

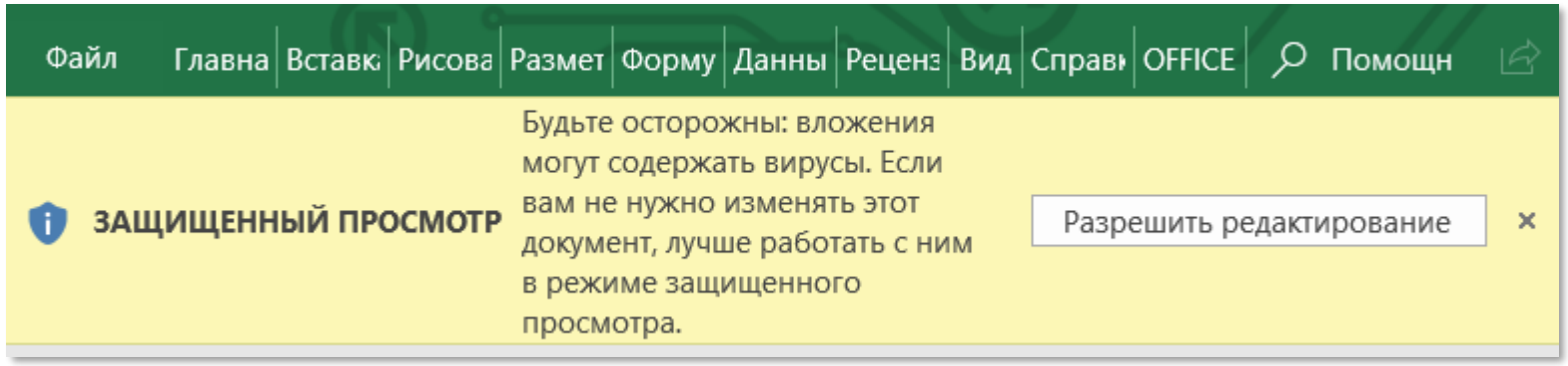
Признаки фишинговых писем

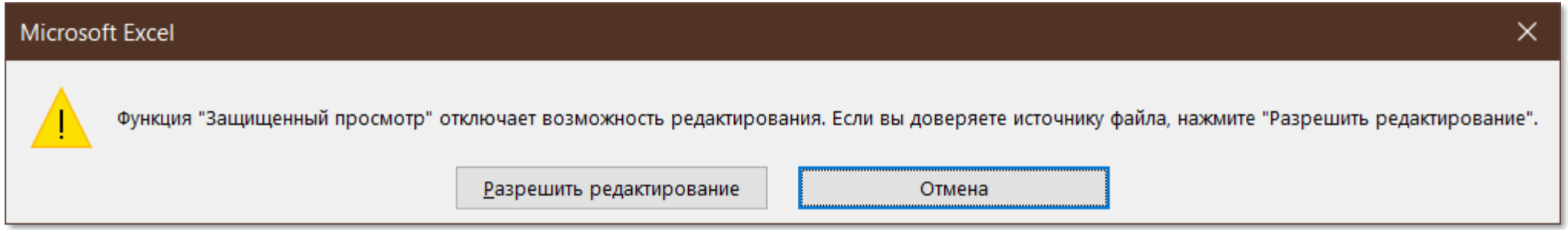
- Все, что нужно злоумышленникам – чтобы вы открыли приложенный к письму файл…



Признаки фишинговых писем (продолжение)

- … или запустили офисный файл с макросом внутри

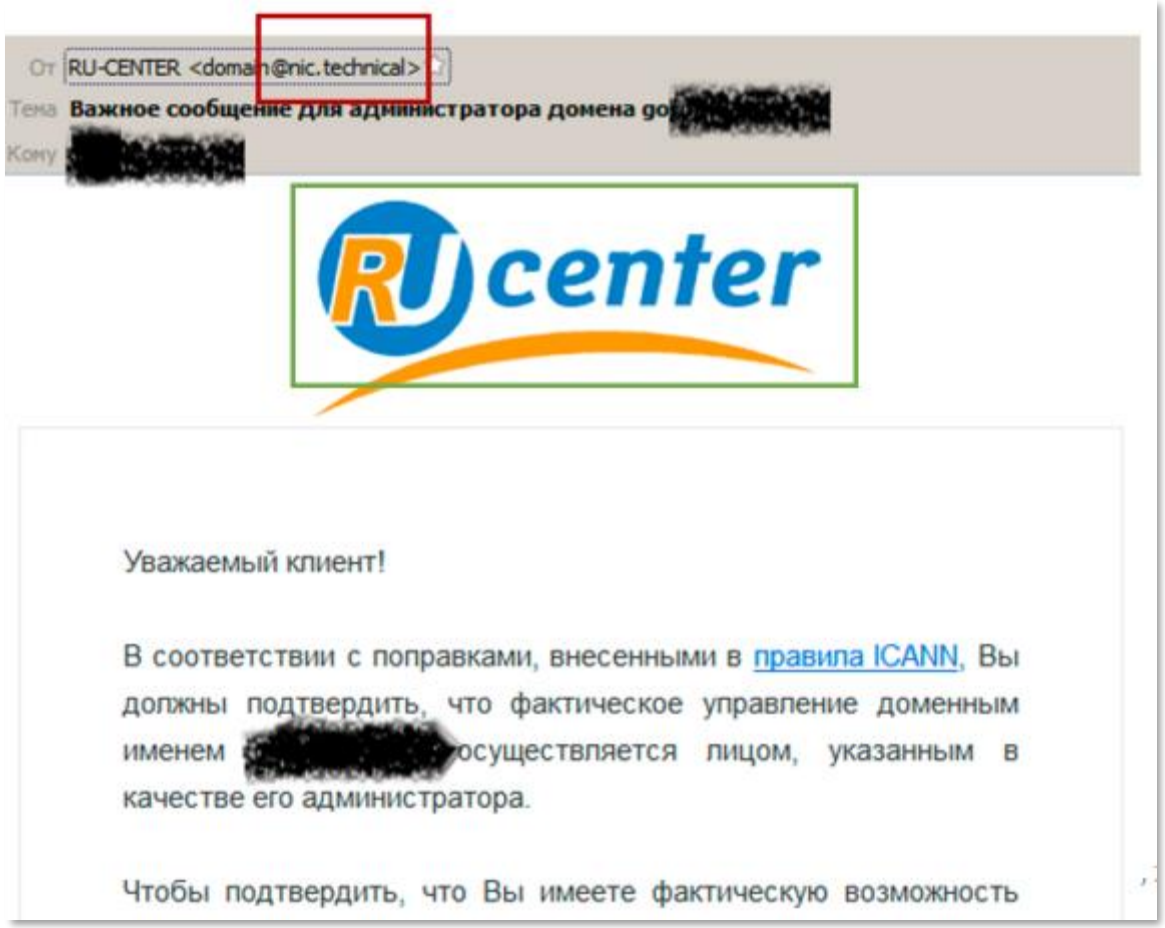




Не разрешайте редактирование и не включайте «содержимое» в чужих файлах!

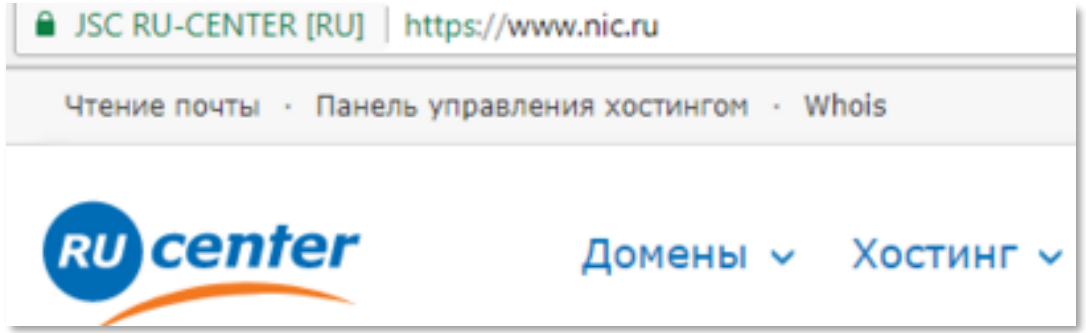
Основные правила защиты от фишинга

1. Обязательно проверять URL-адрес, по которому рекомендуется перейти, на наличие незначительных ошибок в написании



Адрес отправителя находится в домене **nic.technical**

Однако настоящий URL-адрес RU-Center: **nic.ru**



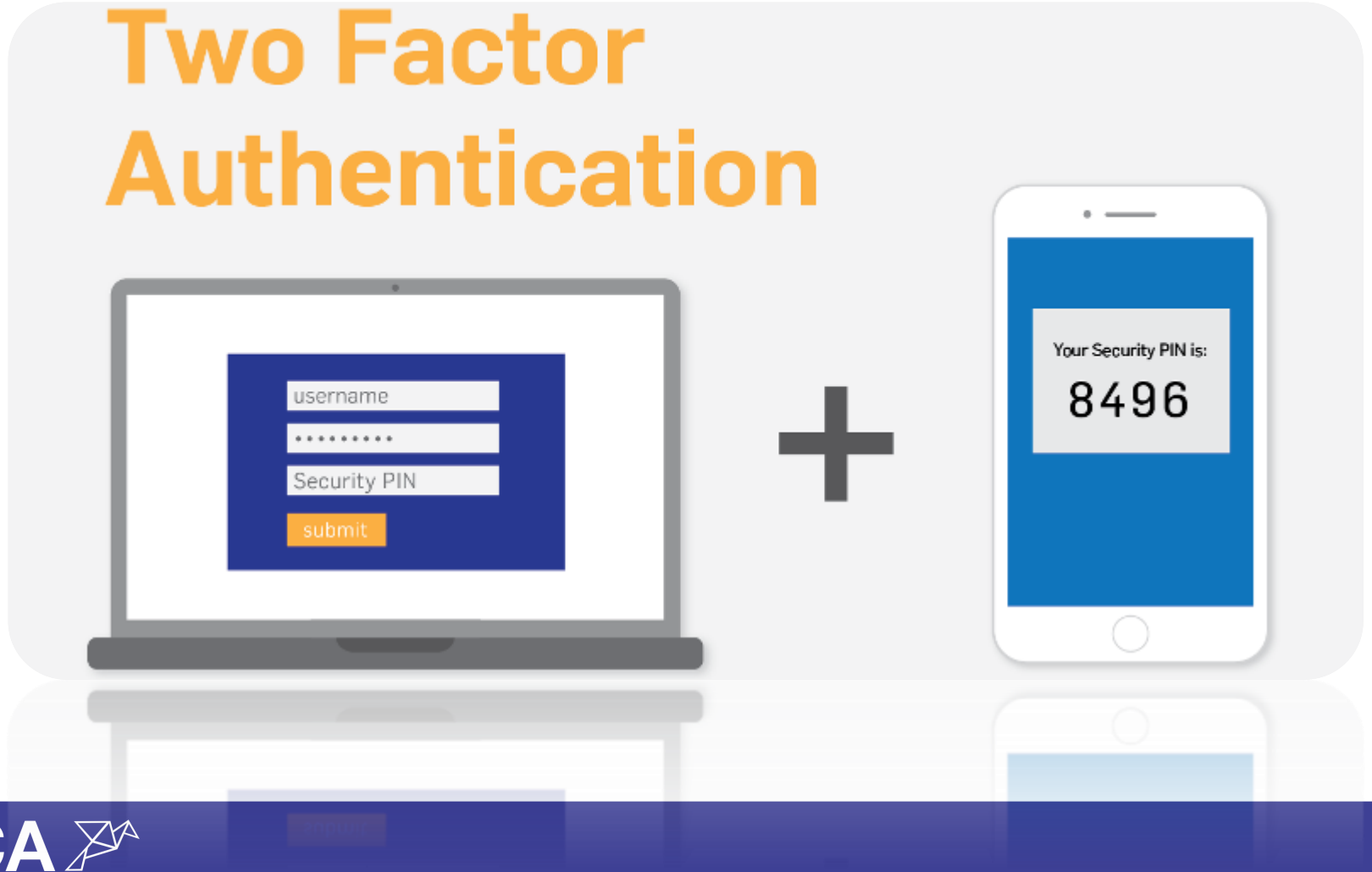
Это письмо от злоумышленника!

Основные правила защиты от фишинга (продолжение)

2. Использовать лишь безопасные https-соединения. Отсутствие всего одной буквы «s» в адресе сайта обязано вас насторожить
3. С подозрением относиться к любым письмам с вложениями и ссылками. Даже если они пришли со знакомого адреса, это не дает гарантии безопасности: он мог быть взломан
4. Получив неожиданное подозрительное сообщение, стоит связаться с отправителем каким-либо альтернативным способом и уточнить, он ли его послал
5. Если все же необходимо посетить ресурс, лучше ввести его адрес вручную или воспользоваться ранее сохраненными закладками
6. Не использовать для доступа к онлайн-банкингу и другим финансовым сервисам открытые Wi-Fi сети: часто их создают злоумышленники. Даже если это не так, подключиться к незащищенному соединению для хакеров не составляет сложности

Основные правила защиты от фишинга (продолжение)

7. На всех аккаунтах, где это возможно, подключить двухфакторную аутентификацию. Эта мера может спасти положение, если основной пароль стал известен злоумышленникам



Выводы и рекомендации

- Обязательно ознакомьтесь с правилами безопасности в сети Интернет и при работе с электронной почтой, а также правилами защиты от фишинга
- Заведите привычку всегда подозрительно относиться к необычным, неожиданным сообщениям и предложениям, а также вбивайте адреса нужных сайтов вручную или пользуйтесь закладками в браузере
- Будьте особенно внимательны к ссылкам и вложениям в письмах

И прежде всего, никому и никогда не передавайте свои пароли!

Стажерская программа

PACIFICA-2019

PACIFICA

Для кого предназначена стажировка?

Требования к кандидатам:

- Выпускники и студенты 3-4-го курсов или магистратуры (по направлению информационная безопасность/информационные технологии)
- Теоретические и практические знания по информационной и кибер-безопасности
- Знание устройства компьютера и локальной вычислительной сети
- Готовность работать полный рабочий день
- Желательно знание языка программирования
- Высокий уровень обучаемости

Условия:

- Стажировка сроком на 3 месяца
- Место стажировки на территории работодателя
- Интересные и ответственные задачи
- Возможность учиться у профессионалов
- **Перспектива трудоустройства в Компанию по окончании стажировки!**

Наши контакты

Алматы	ул. Ауэзова 60, БЦ «Almaty Residence», 6-й этаж, офис 17А тел. +7 (727) 355 00 11
Астана	ул. Д.Кунаева 29/1, гостиница «Дипломат», офис 1906 тел. +7 (7172) 28 00 82
Атырау	ул. Сары Арка 40, офис 230 тел. +7 777 771 79 69
Москва	ул. Верейская, дом 5, 2-й этаж, помещение 1, комната №10 тел. +7 (495) 745 77 88

info@pacifica.kz

facebook.com/pacifica.kz

https://www.pacifica.kz

PACIFICA

www.pacifica.kz