Харківський національний університет
міського господарства імені О.М. Бекетова

Факультет менеджменту

Кафедра Прикладної математики та інформаційних технологій (ПМ та ІТ)

Фішингові атаки. Засоби боротьби з ними.

Автори:
Мартіросян М.К.
Князєв І.А
Керівник:
проф. Новожилова М.В

Харків – Запоріжжя 2017 р.

Що таке фішингова атака?

- Фішинг - (від англ. Fishing рибна ловля, видобування) - вид інтернет шахрайства з використанням соціальної інженерії для отримання доступу до конфіденційної інформації користувачів - логінів і паролів.

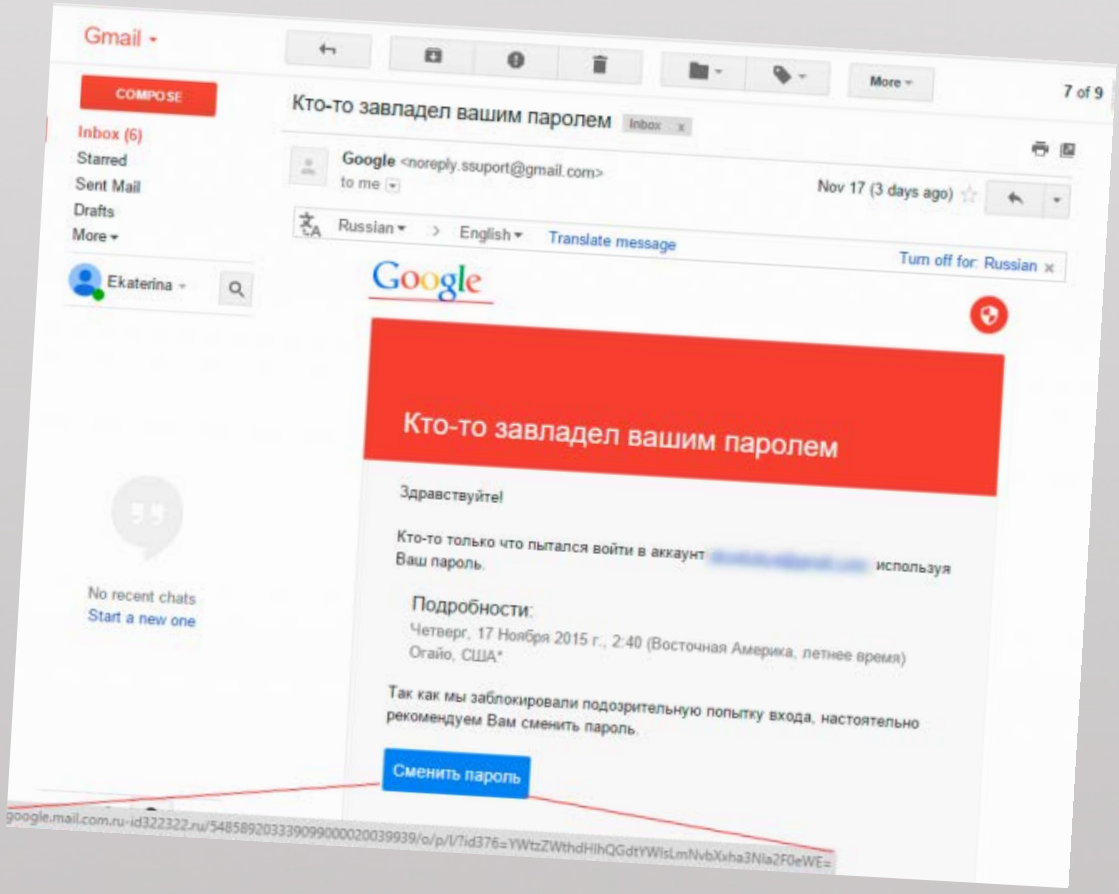
Британський експеримент

- Британська компанія в кав'ярні провела експеримент з кавою.

  Так після цього експерименту , компанії стали більше приділяти уваги захисту конфідеційних даних користувачів.

Як працює інтернет-фішинг?

- Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно.



Приклади схем інтернет-фішингу

- Розсилка підроблених електронних листів, з проханням підтвердити логін і пароль.
- Шахраї створюють електронні листи з підробленим рядком "Mail From:", використовуючи недоліки в поштовому протоколі SMTP.

Приклади схем інтернет-фішингу

- Фіктивні благодійні організації, які звертаються з проханням про пожертвування.
- Створення фішингових інтернет-магазинів.

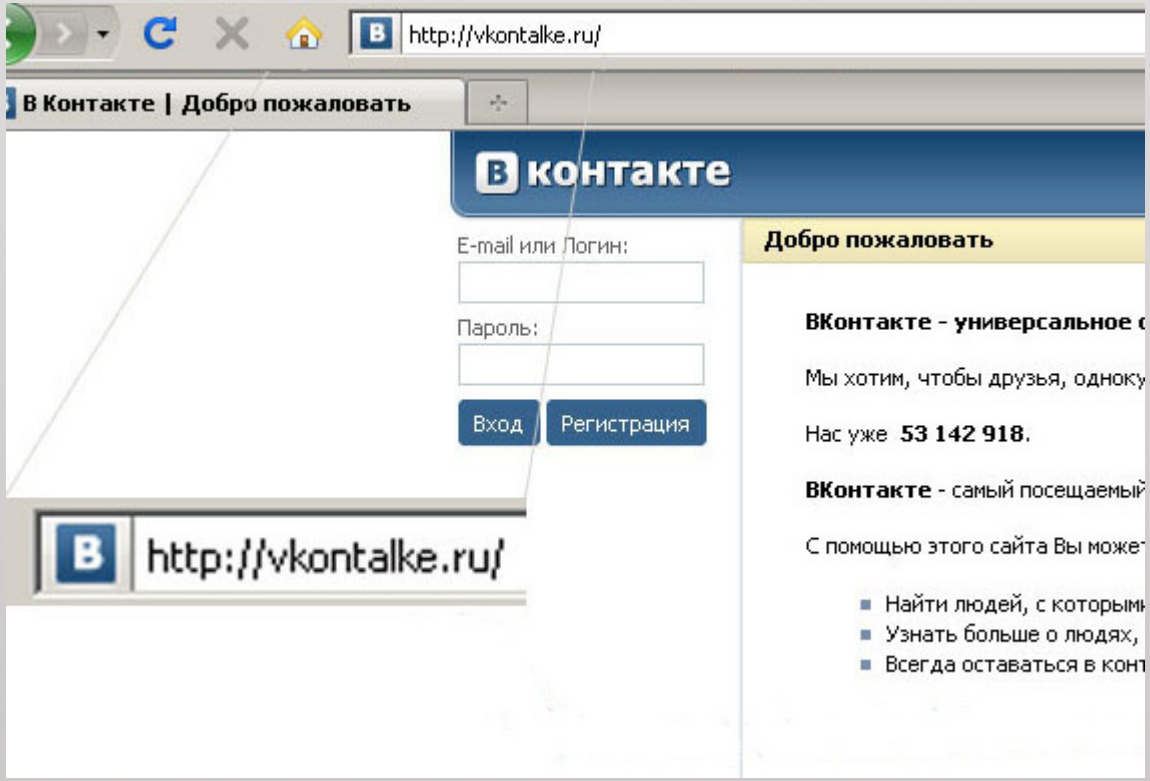
Як розпізнати фішинг?

- На електронну пошту приходить лист, який починається словами «Вітаємо! Ви виграли…". Вам повідомляють про перемогу в розіграші або лотереї, і щоб отримати приз, потрібно всього-то авторизуватися, залишивши на чужому ресурсі дані особистого облікового запису.

Засоби боротьби з фішинговими атаками

- Перш за все, пам'ятайте, що нікому і ні за яких обставин не можна передавати такі конфіденційні дані, як пін-код банківської картки, пароль електронної пошти або акаунтів в соціальних мережах.
- Встановіть хороший антивірус з останньої базою антивірусів.

Засоби боротьби з фішинговими атаками



- Завжди звертайте увагу на дизайн сайту
- Звертайте увагу на адресний рядок на засланні переходу.
- Остерігайтеся заходити на банківські веб-акаунти через точки доступу громадського Wi-Fi

Засоби боротьби з фішинговими атаками

- При відвідуванні банківських сайтів, стежте, щоб було встановлено захищене з'єднання https.
- Якщо виявили фішинговий лист нібито від відомої вам компанії або сервісу, зв’яжіться з ними та повідомте про це в відділення цієї компанії.

Засоби боротьби з фішинговими атаками

- Пропонуємо, один із засобів боротьби з фішинговими атаками. AdBlock - це розширення для веб-браузера. Ця програма не тільки заблокує зайву рекламу, а також попередить про неперевірені сайти. Adblock блокує HTTP-запити відповідно з адресами джерела і може блокувати різні типи елементів сторінки.

Підведемо підсумки

Отже, будьте обережні, слідкуйте за своїми діями у «всесвітній мережі», аби не натрапити на фішингових шахраїв.

Дякуємо за увагу!