Фишинг

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/

Фишинг

Фи́шинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и

История фишинга

- *Техника фишинга была подробно описана в 1987 году, а сам термин появился 2 января 1996 года в новостной группе* alt.online-service.
- *. А уже в 2004 году фишинг стал наибольшей опасностью для компаний, и с тех пор он постоянно развивается и наращивает потенциал.*

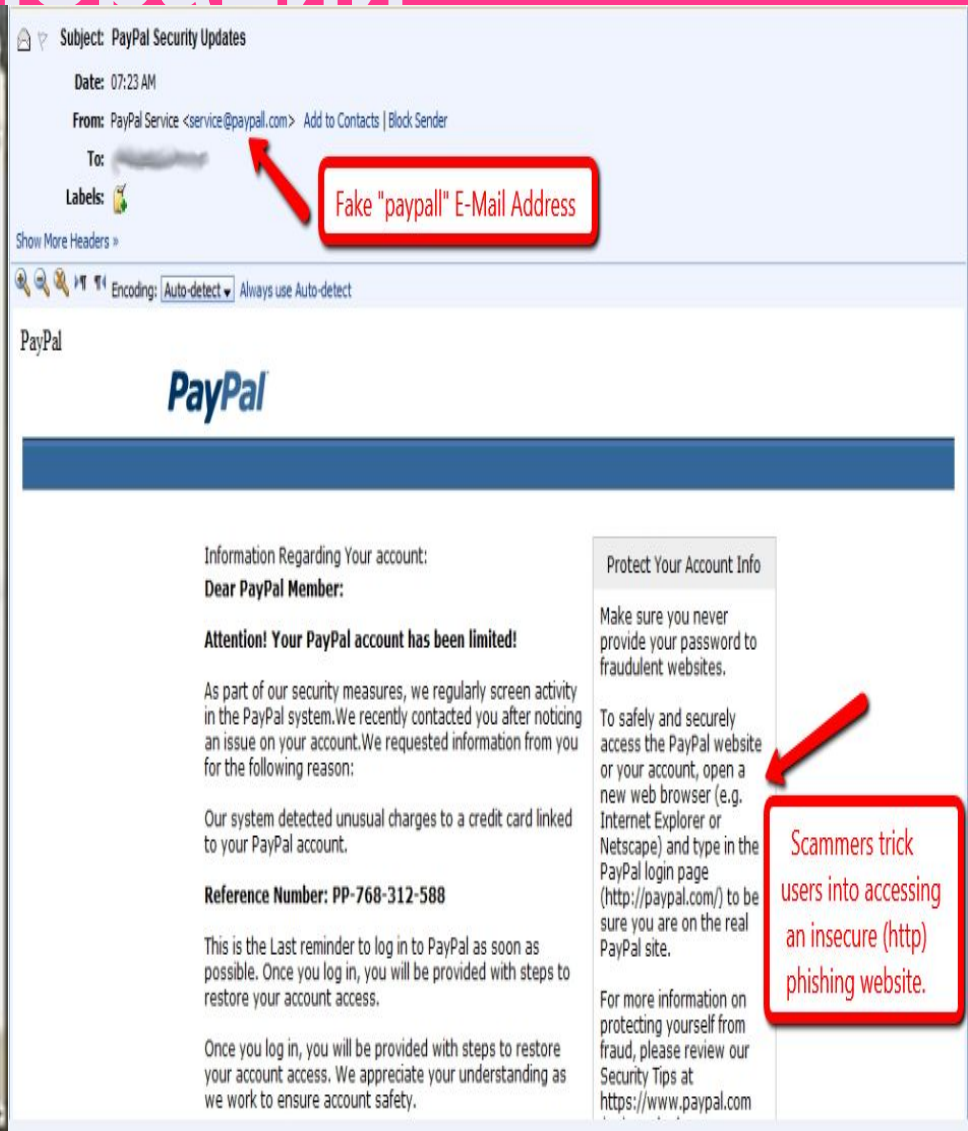
Фишинг сегодня

- *Фишинг стремительно набирает свои обороты, а оценки ущерба сильно разнятся: по данным компании Gartner, в 2004 году жертвы фишеров потеряли 2,4 млрд долларов США[, в 2006 году — ущерб составил 2,8 млрд долларов, в 2007 — 3,2 миллиарда; в одних лишь Соединённых Штатах в 2004 году жертвами фишинга стали 3,5 миллиона человек, к 2008 году число пострадавших от фишинга в США возросло до 5 миллионов*

Методы фишинга

1. *Мошенничество с использованием брендов известных корпораций*
2. *Подложные лотереи*
3. *Ложные антивирусы и программы для обеспечения безопасности*
4. *IVR или телефонный*

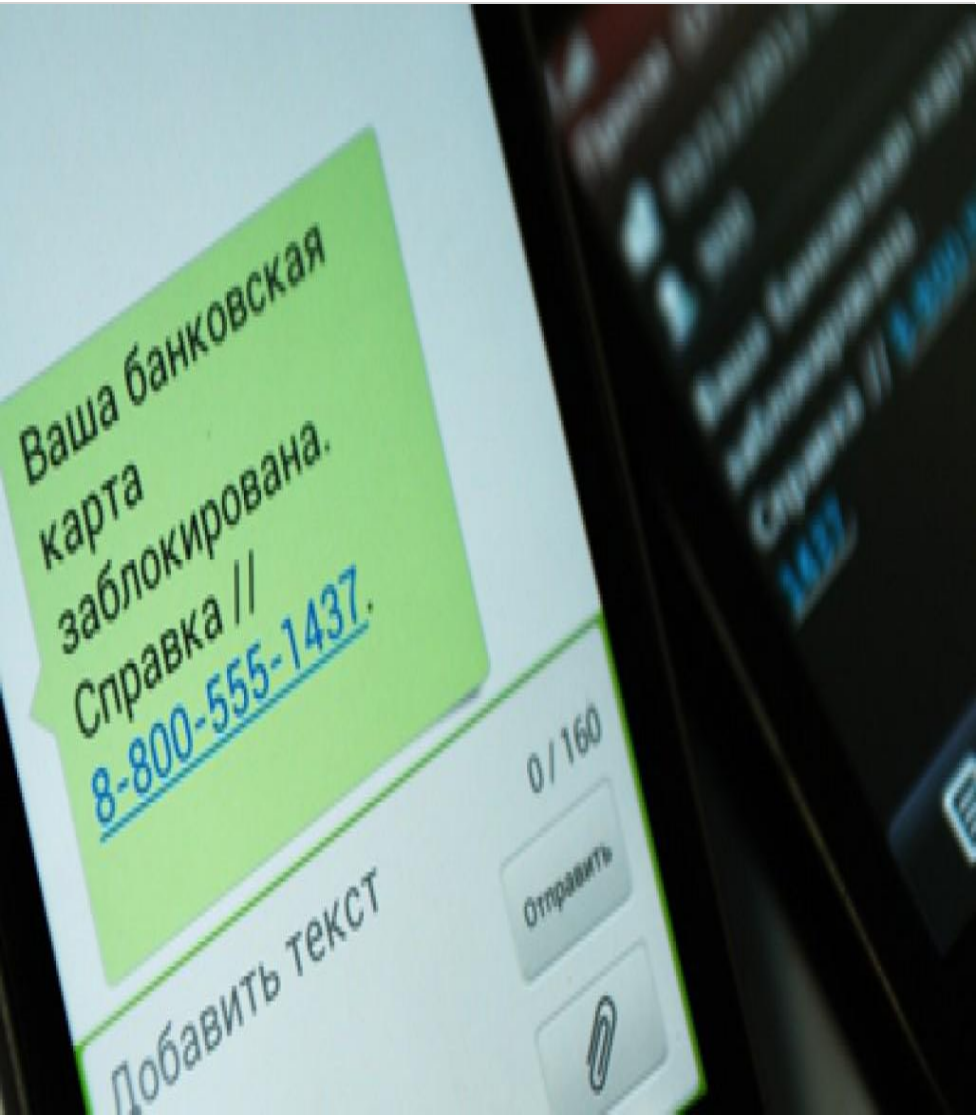
Мошенничество с использованием брендов известных корпораций



Подложные лотереи

- *Письма с уведомлениями о выигрыше в лотерею с регулярностью появляются в электронной почте. Этот вид спама работает по принципу: пользователю сообщают, что он выиграл огромную сумму в лотерее и должен оплатить "предварительные расходы", чтобы ее получить.*

IVR или телефонный фишинг



- *Вишинг– новая форма социотехники, основанная на использовании IP-телефонии (VoIP). Неподозревающий пользователь получает сообщение голосовой почты с указанием перезвонить на номер, принадлежащий легитимной службе банковского самообслуживания. Однако разговор перехватывается мошенником, во владении которого оказываются номера банковских счетов и пароли, сообщаемые по телефону для проверки.*

Ложные антивирусы

- *Ложный антивирус или как его еще называют - лже-антивирус, сегодня является одним из активно набирающих популярность способов Интернет-мошенничества. Суть его заключается в том, чтобы заставить пользователя заплатить деньги за программу, которая якобы удалит с компьютера очень опасные вирусы и защитит в дальнейшем ПК пользователя от различных Интернет-угроз.*

Защита от фишинговых атак

- *Относитесь внимательно к сообщениям, в которых вас просят указать ваши личные данные.*
- *Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных. Убедитесь, что его адрес начинается с "https://" и найдите пиктограмму, похожую на запертый висячий замок, в правом нижнем углу окна браузера.*
- *Не проходите по ссылкам в электронных письмах в формате HTML: киберпреступники могут спрятать адрес подложного сайта в ссылке, которая выглядит как настоящий электронный адрес банка. Вместо этого наберите адрес вручную или скопируйте ссылку в адресную строку браузера.*
- *Убедитесь, что ваше антивирусное решение способно блокировать переход на фишинговые сайты или установите интернет-обозреватель, оснащенный фишинг-фильтром.*
- *Регулярно проверяйте состояние своих банковских счетов и просматривайте банковские выписки, чтобы убедиться в отсутствии "лишних" операций.*
- *Следите за тем, чтобы у вас всегда были последние обновления безопасности*

Источники:

- http://uskof.ucoz.ru/index/fishingovye_ataki/0-55
- https://ru.wikipedia.org/wiki/Фишинг#
- http://www.securitylab.ru/analytics/440661.php
- http://www.phishing.org/history-of-phishing
- http://goo.gl/74YQs