УДК 681.3.06:519.248.681

ОЦЕНКА СТЕПЕНИ УГРОЗЫ И ПУТИ ЗАЩИТЫ ОТ ФИШИНГ-АТАК ИНФОРМАЦИОННОГО ПРОСТРАНСТВА УКРАИНЫ

А.В. Снегуров
Кандидат технических наук, доцент
Кафедра телекоммуникационных систем*
Контактный тел.: 8 (057) 702-10-67
Email: arksn@rambler.ru

Л.О. Макаренко
Контактный тел.: 8-093-763-32-19
Email: oriflamecos@yandex.ru
*Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, г. Харьков, 61166

В статі розглянута проблема фішінга в Україні. Досліджуються причини підвищення небезпеки фішінга, розглядаються напрямки захисту від фішінг-атак.

Ключові слова: фішінг, інформаційна безпека

В статье рассмотрена проблема фишинга в Украине. Исследуются причины увеличения опасности фишинга, рассматриваются направления защиты от фишинг-атак

Ключевые слова: фишинг, информационная безопасность

The problem of fishing in Ukraine is discussed. The causes of increase danger of fishing are investigated, directions of defense from fishing-attacks are considered.t

Key words: phishing, information security

Постановка проблемы

Фишинг-атаки – преступление 21-го века и, по прогнозам аналитиков, это явление может ждать большое будущее. По данным «Лаборатории Касперского» (рис.1) чаще других жертвами фишеров становятся банки, электронные платежные системы и аукционы (лидеры – PayPal и eBay) [1].

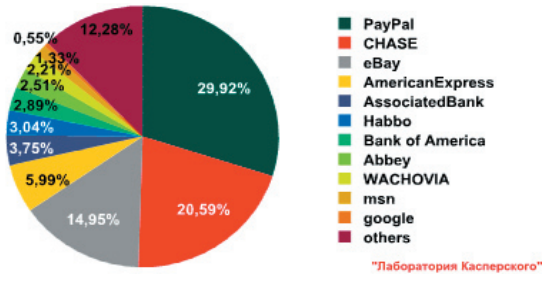

Рис. 1.

В последнее время все более заметным явлением становится так называемый «мобильный фишинг», когда жертву обманом (к примеру, от имени друга или знакомого) заставляют перевести определенную сумму на лицевой счет мошенников. Или в ICQ – когда злоумышленники крадут чужой номер, и потом от лица его владельца рассылают пользователям из контакт-листа просьбы срочно «помочь с деньгами». Сюда же можно отнести и часть сообщений на форумах, в блогах и гостевых книгах с просьбой перечислить деньги «на операцию больному ребенку» с указанием расчетного счета и электронных кошельков, принадлежащих мошенникам. Происходит рассылка в почтовые ящики поддельных счетов на оплату коммунальных услуг.

Кроме финансовых организаций мошенники стали обращать внимание на социальные сети, системы VoIP и почтовые сервисы и на другие типы информационных ресурсов. То есть явление стало распространяться не только интенсивно (за счет новых идей и технологий мошенничества), но и экстенсивно – за счет новых мест для применения этих идей и технологий. Вместе с тем, на банковскую сферу до сих пор приходится подавляющее большинство фишерских атак – более 90%. Так, в США этот вид мошенничества достиг по истине угрожающих размеров: в конце мая 2009 года жертвами фишинга стали, как минимум, 1400 топ-менеджеров крупных компаний, среди которых были и специалисты в области безопасности, например из SecureWorks и Sunbelt Software [2].

Таким образом, фишинг – это, действительно, реально существующая и масштабная проблема, темпы

его распространения соответствуют темпам развития Интернета и распространения интернет-банкинга. В отличие от многих других видов угроз, фишинг обладает четкой ориентированностью на отдельного человека и его финансовые ресурсы. Если существующие средства защиты информации, такие как антивирусы, фаерволы, системы IDS, являются универсальными и подходят как отдельным пользователям, так и компаниям, то с системами защиты от фишинга дело обстоит иначе.

Проблемам анализа деятельности фишеров, способам проведения фишинг-атак, методам защиты от них посвящено огромное количество публикаций. Большое внимание данной проблеме уделяют антивирусные компании («Лаборатория Касперского» и другие), другие организации, занимающиеся информационной безопасностью. Однако проблема фишинга применительно к особенностям украинского информационного пространства является не полностью изученной.

Целью данной статьи является обзор причин повышения опасности фишинг-мошенничества в Украине, обзор методов, используемых злоумышленниками для проведения фишинговых атак, анализ существующих решений, позволяющих противостоять данному виду мошенничества.

Основной материал исследования

На наш взгляд основными причинами, которые повышают опасность фишинг-мошенничества в Украине на настоящий момент времени, являются:

1. Активнейшее развитие Интернета в нашей стране, проникновение его практически во все сферы нашей жизни. Развитие проводных и беспроводных технологий передачи данных (Wi-MAX, Wi-Fi, 3G, 4G), снижение стоимости услуг на пользование Интернетом, делают возможным доступ к данной сети широких слоев населения как в городах, так и сельских районах.

2. Стремительный рост рынка электронных платежей на постсоветском пространстве. Так, например, по результатам 2008 года оборот электронных платежей в Украине через систему WebMoney Transfer (по разным оценкам, осуществляющую 85 – 90% оборота электронных платежей по Украине) достиг 663 млн. гривен, что практически в 3 раза превысило данные показатели по 2007 году. По состоянию на 1 января 2009 года в системе было зарегистрировано 1 млн. 370 тыс. человек, объем осуществленных транзакций превысил 3,5 млн. [3]. Бурный рост системы электронных платежей происходит и у наших ближайших соседей, что также влияет на ситуацию в данной сфере в Украине [4].

3. Критически низкий уровень грамотности в сфере информационной безопасности населения Украины. Так, авторами для понимания ситуации был проведен опрос нескольких сотрудников одной из крупнейших финансовых организаций Украины. Ответить на вопрос «что такое фишинг?» не сумел не один. Данную проблему подтверждают и ведущие информационно-аналитические источники по информационной безопасности [5]. А что говорить об остальной части населения нашей страны («домашних пользователей»)? Также необходимо учитывать, что сейчас легко можно собрать персональную информацию через социальные сети «В контакте», «Одноклассники» и другие.

4. Вхождение Украины в информационно-культурную жизнь европейского сообщества, проведение на территории Украины крупнейших общеевропейских мероприятий. В качестве примера подобного мероприятия можно отметить планирование проведения в нашей стране чемпионата Европы по футболу Евро-2012. Такое мероприятие вполне может быть использовано злоумышленниками для проведения фишинга. В мире уже имеются подобные примеры фишинг-атак. Так во время подготовки к проведению чемпионата мира по футболу в 2006 году мошенники рассылали электронные письма от имени комитета ФИФА по организации мирового футбольного первенства. Отправители писем извещали получателей о выигрыше в лотерее и просили для получения денег сообщить свои персональные данные, в том числе, данные о банковском счете [6]. Данная рассылка писем состоялась через несколько месяцев после рассылки вредоносной программы в письме с информацией о бесплатных билетах на матчи чемпионата. Кроме того, клиентам сразу нескольких бразильских банков фишеры рассылали письма от имени платежной системы Mastercard и предлагали пользователям возможность бесплатно отправиться в Германию и посетить несколько матчей мирового первенства. Для того чтобы использовать эту возможность, получатели писем должны были перейти по вставленной в письмо ссылке. Однако клик в итоге загружал на компьютер программу для считывания логов клавиатуры. В результате, когда пользователь посещал банковские сайты с компьютера с установленной вредоносной программой, его логин и пароль оказывались в руках у фишеров. В числе фишерского списка сайтов оказались bradesco.com.br, itau.com.br, unibanco.com.br, bancoreal.com.br, caixa.gov.br и caixa.com.br [7].

Таким образом, фишинг, в настоящее время, представляет реальную угрозу для граждан Украины.

Итак, фишинг – это процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют spam или компьютеры-боты. Фишинг нападения полагаются на соединение методов технического обмана и факторов социальной инженерии. В большинстве случаев фишер должен убедить жертву преднамеренно выполнить ряд действий, которые обеспечат доступ к конфиденциальной информации.

Рассмотрим известные способы реализации фишинг-атак.

1. Использование электронной почты и Spam. Наиболее распространены фишинговые атаки, проводимые с использованием электронной почты. Используя методы и инструментальные средства спамеров, фишеры могут создать специально созданные электронные сообщения миллионам законных адресов электронной почты в течение нескольких часов (или минут, используя распределенные бот-сети). Методы, используемые фишерами при работе с электронной почтой:

• Официальный вид письма. Так, например, ходе своего исследования американские специалисты провели работу с фокус-группами. 90 процентов участников фокус-групп оказались неспособными понять, пришло им подлинное или фальшивое письмо. Ис-

следователи представили респондентам хорошо подделанное письмо от банка Bank Of the West, в котором стояла ссылка на фишинг-сайт www.bankofthevvest.com (с двойной «v» вместо «w»). Сайт содержал все элементы, способные ввести пользователей в заблуждение: символ замка, лого компании VeriSign и даже pop-up с предупреждением о необходимости соблюдать правила безопасности [8].

• Копирование законных корпоративных адресов электронной почты с незначительными изменениями URL;

• Стандартные вложения вируса в сообщения;

• Обработка уникальных почтовых сообщений;

• Поддельные отсылки по почте к популярным доскам объявлений и спискам адресатов;

• Использование поддельной строки “Mail From:” адреса и открытые почтовые релеи маскируют источник электронной почты и другие.

2. Проведение фишинг-атак с использованием web-контента. Данный метод фишинг атак заключается в использовании злонамеренного содержания web-сайта. Это содержание может быть включено в сайт фишера, или сторонний сайт. Доступные методы доставки контента включают:

• Включение HTML замаскировывающее ссылки в пределах популярных сайтов;

• Использование сторонних включений или заголовков рекламных банеров для соблазнения клиентов к посещению фишерского сайта;

• Использование дефектов сети, чтобы проследить потенциального клиента в подготовке к нападению фишеров;

• Использование всплывающих окон, чтобы замаскировать истинный источник фишерского сообщения;

• Внедрение злонамеренного содержания в пределах просматриваемой web-страницы, которая эксплуатирует известную уязвимость в пределах программного обеспечения web-браузера клиентов и устанавливает программное обеспечение фишера (например, троянские программы).

3. Фальсификация рекламных баннеров. Реклама с помощью банера - очень простой метод фишинга. Он может использоваться для переадресации клиента к поддельному сайту организации.

4. IRC и передача IM-сообщений. Можно предположить, что количество фишинг-атак с использованием этих технологий будет резко увеличиваться.

5. Использование троянских программ. В то время как среда передачи для фишинг-атак может быть различна, источник атаки все чаще оказывается предварительно скомпрометированным домашним ПК. При этом как часть процесса компрометации используется установка троянской программы, которое позволит фишеру использовать персональные компьютеры в качестве распространителей вредоносных сообщений.

Специалистами по информационной безопасности разработаны эффективные методы борьбы с фишинг-атаками. Необходимо отметить, что организации, занимающиеся электронными платежами, используют методы защиты, взломать которые очень сложно. Например, система WebMoney применяет аутентификацию с использованием токенов, многофакторную аутентификацию (пароль+файл+ключ), шифрование данных алгоритмом типа RSA, ключом 1024 бит, и другие средства защиты [9]. Однако уязвимым элементом систем электронных платежей является клиент. Именно некомпетентность пользователей данных систем приводит к высокой эффективности фишинг-атак.

Поэтому методы защиты от фишинг-атак можно разделить на две больших категории:

1. Методы социальной инженерии.

2. Технические методы.

К техническим методам можно отнести использование программных антивирусных программных продуктов, осуществляющих защиту от троянских программ, так называемых антифишинговых фильтров ведущих антивирусных компаний („Лаборатории Касперского”, Symantec и других).

Однако в первую очередь на эффективность борьбы с фишингом влияют методы социальной инженерии, к которым необходимо отнести:

- обучение вопросам защиты от кибер-преступности, в том числе и от фишинг-атак, персонала коммерческих организаций, использующих системы электронных платежей;

- повышение грамотности в сфере информационной безопасности широких слоев населения нашей страны;

- подготовка специалистов в сфере информационной безопасности.

Выводы

В настоящее время создан ряд предпосылок для обострения проблемы фишинга в Украине. Необходимо проведение эффективных мероприятий по защите пользователей глобальной сети от фишинг-мошенничества, в первую очередь, таких как, обучение вопросам защиты от фишинг-атак.

Литература

1. Kaspersky Security Bulletin. Спам в 2008 г. [Электронный ресурс] / Viruslist.com. Інтернет – безопасность. – Режим доступа: URL: http://www.viruslist.com/ru/analysis?pubid=204007646#9/ - 3.02.2009г. – Загл. с экрана.
2. Хакеры запугали 1400 топ-менеджеров. [Электронный ресурс] / CNEWS. Издание о высоких технологиях. - Режим доступа: URL: http://www.cnews.ru/news/top/index.shtml?2007/05/31/252845) – 31.05.2007г. – Загл. с экрана.
3. WebMoney Transfer – итоги 2008 года в Украине [Электронный ресурс] / Kiosksoft. Программное обеспечение и платежные системы. – Режим доступа: URL: http://kiosksoft.com.ua/news/278.html/ - 2.2.2009г. – Загл. с экрана.
4. Россию ждет взрывной рост рынка интернет-платежей [Электронный ресурс] / Деловая пресса. – Режим доступа: URL: http://www.businesspress.ru/ newspaper/article_mId_ 6187_aId_446965.html/ - 18.4.2008г. – Загл. с экрана.
5. Данилов М.П. Самая опасная уязвимость / М.П. Данилов // Защита информации. INSIDE. - 2006. - № 6. – С. 32 – 35.
6. Игорь Громов. Интернет-мошенники провели лотерею от имени ФИФА [Электронный ресурс] / Viruslist.com.

Інтернет – безопасность. – Режим доступа: URL: http://www.viruslist.com/ru/news?id=171007177 - 30.09.2005г. – Загл. с экрана.
7. Игорь Громов. Фишеры заманивают бразильцев на чемпионат мира по футболу [Электронный ресурс] / Viruslist.com. Інтернет – безопасность. – Режим доступа: URL: http://www.viruslist.com/ru/news?id=183341093 - 30.04.2006г. – Загл. с экрана.
8. Игорь Громов. Американские академики раскрыли секреты успеха фишеров / Viruslist.com. Інтернет – безопасность. – Режим доступа: URL: http://www.viruslist.com/ru/news?id=183389068 - 4.04.2006г. – Загл. с экрана.
9.Электронные платежи: риски и безопасность [Электронный ресурс] / Prostobank – Режим доступа: URL: http://www.prostobankir.com.ua /it/stati/elektronnye_platezhi_riski_i_bezopasnost/ - 17.07.2008г. – Загл. с экрана.

Розглядається деяка концепція системного підходу до створення сучасних інформаційних систем маркетингу (ІСМ) підприємств, яка враховує багатоцільове спрямування ІСМ та їх комунікативне призначення. Передбачається обґрунтування принципів побудови засобів концептуальної комплексної багатоцільової функціональної архітектури ІСМ з використанням сучасних засобів Інтернет-технологій

Ключові слова: системний підхід, інформаційні системи маркетингу, Інтернет технології

Рассматривается некоторая концепция системного подхода к созданию современных информационных систем маркетинга (ИСМ) предприятий, которая учитывает многоцелевое направление ИСМ и их коммуникативное назначение. Предусматривается обоснование принципов построения средств концептуальной комплексной многоцелевой функциональной архитектуры ИСМ с использованием современных средств Интернет-технологий

Ключевые слова: системный подход, информационные системы маркетинга, Интернет технологии

Some conception of systems approach to creation of the modern informative systems of marketing (ISM) of enterprises is considered, which takes into account the mnogotselevoe direction ISM and their kommunikativnoe setting. The ground of principles of construction of facilities of the conceptual complex mnogotselevoy functional architecture ISM with the use of modern facilities of Internettechnologies is foreseen

Key words: systems approach, informative systems of marketing, the Internet of technology

УДК 656:621.3

КОНЦЕПЦІЯ СТВОРЕННЯ ТА РОЗВИТКУ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ МАРКЕТИНГУ ПІДПРИЄМСТВ

В.Б. Задоров
Кандидат технічних наук, професор, завідуючий кафедрою*

К.І. Київська
Аспірант*
Контактний тел.: 8 (096) 703-83-15
E-mail: kiev_katya@mail.ru
*Кафедра інформаційних технологій
Київський національний університет будівництва та архітектури
пр. Повітрофлотський, 31, м. Київ ,Україна

1. Вступ

Сучасний стан і стрімкий розвиток засобів інформаційних технологій створюють нові умови для створення і розвитку інформаційних управляючих систем підприємств. Ці нові умови, насамперед, пов'язані зі зміною системних поглядів на інформаційну складову сучасних підприємств, яка за своєю важливістю (а іноді і вартістю) швидко зростає в порівняні з іншими господарськими ресурсами. Зміни в системному по-