УДК 343.918

ОСТОРОЖНО, ФИШИНГ!

Хачатурова С.С., Жихарева Ю.П.

ФГБОУ ВО «Российский экономический университет имени Г.В. Плеханова», Москва, seda_@mail.ru

Информатизация нашего общества продолжается в достаточно быстром темпе. Пользователей информационными технологиями становится все больше. Вместе с этим возрастает и число кибератак, то есть информационных преступлений, в частности, фишинговых атак. В данной статье мы рассмотрели актуальное на сегодняшний день информационное преступление – фишинг. Проанализировали существующие сегодня проблемы выявления, устранения, профилактики таких преступлений и определили какие существуют способы борьбы с киберпреступностью, в частности, с фишингом. Дали определение данному значению. Сделали вывод, что помимо правовых механизмов борьбы с фишингом, важную роль играет и поведение самого человека. Рассмотрели, какие механизмы решения данной проблемы существует сегодня у нашего государства. Достаточно большого количества фишинговых атак можно избежать, если знать базовые правила безопасного использования информационных электронных систем.

Ключевые слова: фишинг, кибератака, киберпреступление, свишинг, преступление, право, закон, уголовный, проблема, взлом, информационные, технологии, атака

BEWARE OF PHISHING!

Khachaturova S.S., Zhikhareva Y.P.

Plekhanov Russian University of Economics, Moscow, e-mail: seda_@mail.ru

Computerization of our society continues at a fast enough rate. Users of information technology becomes more and more. Along with this increase in the number of cyber-attacks, that is, information crimes, particularly phishing attacks. In this article, we reviewed relevant today information crime is phishing. Analyzed existing problems of detection, elimination, prevention of such crimes and identified what are the ways to combat cyber-crime, in particular phishing. Given the definition of this value. Concluded that in addition to legal mechanisms to combat phishing, plays an important role and behavior of the person. Examined the mechanisms of solution of this problem exists today in our state. A sufficiently large number of phishing attacks can be avoided if you know the basic rules for secure use of electronic information systems.

Keywords: phishing, cyber-attack, cyber-crime, phishing, crime, law, law, criminal, problem, hacking, information, technology, attack

Такое бывает в нашей жизни: живешь…, в будни ходишь на работу, а в выходные вместе с семьей или друзьями ходишь в кино или в театр и, конечно же, откладываешь по возможности деньги на отдых, поездку, обучение или на покупку необходимого.

А мошенники тем временем тоже не бездействуют. Они, используя современные информационные технологии могут быстро и без затруднений лишить *жертву* собственных электронных денег...

В данной статье мы хотели рассмотреть данное актуальное на сегодняшний день информационное преступление – *фишинг*. А также проанализировать существующие сегодня проблемы выявления, устранения, профилактики таких преступлений и определить, какие существуют способы борьбы с киберпреступностью, в частности, с фишингом.

Для начала дадим определение, что же такое ***фишинг***. Итак, это один из большого количества видов компьютерных или киберпреступлений, то есть разновидность компьютерного мошенничества. Суть фишинга заключается в том, что киберпреступники (их также называют фишерами) стремятся посредством компьютерных технологий завладеть личными данными обычных людей (пользователей интернета) и, используя эти данные, завладеть средствами пользователей.

Фишеры используют самые разнообразные и изощренные методы для достижения своих целей. Например, можно создать сайт, внешне неотличимый от сайта какого-либо известного банка или фирмы. Все пользователи, которые зайдут на поддельный сайт, введут свои данные: пароль, регистрационное имя, PIN – код и т.п. Таким образом, они дают мошенникам ключ к своим денежным средствам. Распространенным приемом у фишеров также является рассылка электронных сообщений пользователям с уведомлением, например, что их организация проводит какие-то изменения для проверки безопасности или же, что пользователь является должником данной организации. Приемов достаточно много, но все они направлены на достижение единой цели – фишеру необходимо завладеть личными данными пользователя, и, фактически, если пользователь поверит рассылке, не проверит данный сайт и пройдет по гиперссылке,

указанной в электронном письме или даже просто откроет это письмо, он становится жертвой мошенничества.

Так как информатизация нашего общества продолжается в достаточно быстром темпе, пользователей информационными технологиями становится все больше. Вместе с этим возрастает и число *кибератак*, то есть информационных преступлений, в частности, фишинговых атак.

На ранних этапах развития этого вида мошенничества фишеры пользовались системами мгновенных сообщений, пытаясь уговорить жертву предоставить личные данные, и использовали ее данные для распространения спама, жертвами большей частью становились обычные пользователи при том условии, что не у всех людей на тот момент были счета в банках. Но сегодня, с развитием электронной платежной системы и иных информационных технологий, в группу риска попадают как обычные пользователи и их средства, так как у большей части людей сегодня есть банковские дебетные или кредитные карты, счета в банках и т.п. Из этого следует, что возрастает количество электронных денег, а значит – и количество фишеров, и масштаб совершаемых ими преступлений. Это, на сегодняшний день является *актуальной проблемой*.

По оценкам экспертов, из всех случаев незаконного использования банковских карт, 57% случаев – результат фишинга. Чаще всего атаки совершаются в отношении банков и иных кредитных организаций. Потерянные суммы денег достигают миллионов рублей. По данным компании FICO, Россия занимает пятое место в мире по потерям от преступлений с кредитными картами.

Теперь давайте рассмотрим, какие механизмы решения данной проблемы существуют у государства на сегодняшний день.

Так как первые известные случаи фишинговых атак произошли в Америке, то и законодательство в этой сфере развивается там быстрее, чем в прочих странах. Американское законодательство в начале 2000-х столкнулось с несколькими *громкими* случаями кибератак, в результате которых оказались похищены крупные суммы денег. Это побудило власть начать разрабатывать законодательство в сфере информационной преступности. На сегодняшний день американское антифишинговое законодательство дает пользователям информационных систем гарантии того, что преступники в данной сфере понесут суровое наказание за свои действия, т.к. меры наказания за данную категорию преступлений выработаны достаточно жесткие: фишеров обязывают платить достаточно крупные штрафы, а в некоторых случаях им может грозить и лишение свободы. Например, в 2007 году палата представителей США приняла законопроект, в соответствии с которым фишерам, незаконно использующим персональные данные людей, грозит до 2-х лет лишения свободы, а использование преступниками шпионских программ карается сроком до 5 лет.

Такие законопроекты являются результатом правотворческой деятельности США и действуют только на ее территории. В РФ ситуация с законодательством в сфере информационной преступности находится не на самой высокой ступени своего развития. Когда в России начали происходить фишинговые атаки (первое громкое дело против фишеров началось в 2009 г.: преступники похитили около 6 млн рублей), фишеры несли ответственность за неправомерный доступ к чужой информации, а также за мошенничество, а не за конкретное преступление – не за фишинг.

С помощью фишинга в России осуществляется около 70% всех несанкционированных операций с применением платежных карт, а в законодательстве отсутствует уголовная ответственность за фишинг. Существуют статьи, предусматривающие ответственность за изготовление и сбыт фальшивых банковских карт и других платежных документов, предусматривающие наказание за мошенничество. Но статья, которая четко обозначала фишинг, как одну из разновидностей преступлений, и предусматривала соответствующее наказание за такие преступления в Уголовном кодексе РФ, отсутствует.

Известно, что в 2015г. в Государственной думе обсуждался законопроект о введении уголовной ответственности за фишинг, однако, несмотря на бурные дискуссии и видимое одобрение законопроекта, конкретных мер к его реализации пока не принято. Более того, четкого определения *фишинг* в Российском законодательстве не существует. Нет не только уголовной ответственности за этот вид киберпреступности, хотя порой вред от них достаточно весомый, ответственности именно за совершение *преступления-фишинг* в наших законах нет.

Кроме того, помимо несовершенств в законодательстве, существует ряд иных проблем в обнаружении, расследовании и предотвращении фишинга. Во-первых, фишеры воздействуют на психологию человека. Это значит, что фишер не подходит к вам с ножом и не требует сказать пароль от банковской карты, он действует более осторожно, что требует больших навыков, некоторой подготовки и определенного опыта.

Все это, на наш взгляд, может рассматриваться как отягчающие обстоятельства при расследовании фишинговых преступлений. Практика рассылки множества провокационных электронных сообщений, совершение звонков с сообщениями о каких-то трагических событиях (здесь имеют место такие разновидности фишинга, как *свишинг* – то есть фишинг посредством сообщений; и *вишинг*- фишинг посредством звонков пользователям. Все это приводит к тому, что человек под влиянием эмоций, совершает действия, последствий которых он в данный момент не может предусмотреть, и фишеры пользуются этим.

Из этого мы можем сделать вывод, что помимо правовых механизмов борьбы с фишингом, важную роль играет и поведение самого человека. Достаточно большого количества фишинговых атак можно избежать, если знать базовые правила безопасного использования информационных электронных систем. Человек должен внимательно просматривать адрес сайтов, с которых ему приходят сообщения, по возможности проверять их подлинность. Крупные организации предусматривают возможность фишинговых атак, поэтому предупреждают пользователей о возможных угрозах, а также сами стараются предоставить доказательства подлинности. Некоторые сайты, при рассылке своим пользователям сообщений, могут указывать какой-либо фрагмент персональных данных пользователя, как доказательство. Значит, ознакомление людей с правилами безопасного использования интернета, электронных платежных систем, да даже и обычного поиска в интернете, могут значительно снизить уровень ущерба, причиняемого фишерами.

Другой момент – сегодня информационные технологии развиты настолько, что фишеры могут овладевать нужной им информацией практически без участия пользователя. Например, это случаи, когда человек регистрируется на официальном сайте, где фишер заранее устанавливает на ней специальную *программу-шпион*, которая фиксирует информацию о каждом пользователе. И если какой-то пользователь зарегистрировался на этом *зараженном* сайте, все его данные могут быть использованы фишером, и он может лишиться средств на своей карточке, более того, обнаружить, что должен какому-либо банку достаточно крупную сумму денег. Решения этой проблемы также на 100% сегодня не существует. Компании тратят внушительные средства на разработку антифишингового программного обеспечения, что является определенной гарантией безопасности как для людей, пользующихся услугами данной организации, так и для самих организаций, потому что объем денежных средств отдельного пользователя чаще всего несоизмеримо мал по сравнению с активами крупных организаций.

Из всего сказанного выше мы можем сделать несколько выводов:

1. Специфика данного преступления требует особого анализа с нескольких сторон:

- с *психологической*, т.к. идет непосредственное воздействие на человеческую психику и об определенной степени морального вреда, который может быть нанесен человеку в результате кибератаки,
- с *юридической*, так как мы говорим о нарушении определенных человеческих прав, прав на защиту персональных данных, на личную информацию.
- с экономической, так как вред, причиняемый фишером, вред материальный; ведь цель фишинга – получить определенные денежные средства.

2. В данной ситуации в роли потерпевшей стороны может оказаться любой субъект – обычный человек, организация, а возможно, что и государство, значит данная проблема является особенно важной для общества и актуальной в наше время, и каждый заинтересован в ее решении.

Пока еще рано говорить о том, сможем ли мы победить и окончательно ликвидировать фишинг из нашего общества, потому что развитие новых информационных технологий сейчас в стадии быстрого развития и предугадать, какие новые знания мы получим завтра и как они нам помогут, мы не можем. У нас пока нет компетентного законодательства для наказания фишеров, недостаточно специалистов в области информационного права, а наши развивающиеся информационные технологии пока не в состоянии обогнать развитие техник фишинга.

В этой статье мы выделили основные направления мер безопасности, которые в будущем должны нам помочь избавиться от этой злободневной проблемы.

Остерегайтесь фишинга!

Список литературы

1. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991.

2. Ведеев Д.В. Защита данных в компьютерных сетях. – М.: Открытые системы, 2001. – № 3.

3. Хачатурова С.С. Информационные технологии в юриспруденции (Учебное пособие). Фундаментальные исследования. – 2009. – № 9. – С. 8–9.

4. Хачатурова С.С. Хранение и зашита информации. Международный журнал прикладных и фундаментальных исследований. – 2016. – № 2–1. – С. 63–65.

5. Мандиа К., Просис К. Расследование компьютерных преступлений. Лори. 2005.

6. Джеймс Л. Фишинг. Техника компьютерных преступлений. НТ Пресс. 2008.