7. ГОСТ Р ИСО 9 241-210-2012 Эргономика взаимодействия человек–система. Часть 210. Человеко-ориентированное проектирование. — Введ. 29.11.2012. — М.: Стандартинформ, 2013. — 36 с.

8. Филимонов В.В. Экспрессия и упорядоченность в письменной речи / В.В. Филимонов, А.А. Живодеров, Л.Г. Горбич // Известия УрФУ. Серия 1 Проблемы образования, науки и культуры. — 2012. — №3 (104). — С. 313–319.

9. Филимонов В.В. Кластеризация русскоязычных текстов с применением статистики χ^2 / В.В Филимонов, А.М. Амиева, А.П. Сергеев // Информационные технологии, телекоммуникации и системы управления: материалы Международной научно-практической конференции, 12–13 января 2016 г., г. Екатеринбург. / УрФУ имени первого Президента России Б.Н. Ельцина, Екатеринбург, 2016. — С. 164–174.

10. Филимонов В.В. Атрибутирование русскоязычных текстов с использованием закона больших чисел / В.В. Филимонов, А.М. Амиева, А.А. Живодёров, А.А. Крамаренко // Информационные технологии, телекоммуникации и системы управления: материалы Международной научно-практической конференции, 12–13 января 2017 г., г. Екатеринбург. / УрФУ имени первого Президента России Б.Н. Ельцина, Екатеринбург, 2017 — [в печати].

11. Крамаренко А.А. Применение модели случайных блужданий для описания русскоязычных текстов / А.А. Крамаренко, В.В. Филимонов, А.А. Живодёров, А.М. Амиева // Информационные технологии, телекоммуникации и системы управления: материалы Международной научно-практической конференции, 12–13 января 2017 г., г. Екатеринбург. / УрФУ имени первого Президента России Б.Н. Ельцина, Екатеринбург, 2017 — [в печати].

УДК 316.77:004

Д.А. Богданова

О НЕКОТОРЫХ ПОСЛЕДСТВИЯХ КРАЖИ ИДЕНТИЧНОСТИ

Богданова Диана Александровна
d.a.bogdanova@mail.ru
Институт образовательной информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук, Россия, г. Москва

ON SOME OF THE CONSEQUENCES OF IDENTITY THEFT

Bogdanova Diana Aleksandrovna
Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Russia, Moscow

Аннотация. *Рассматривается последствие кражи идентичности в социальной сети, приводящая к созданию фальшивых профилей. Впоследствии эти профили используются для мошеннических действий- любовных афер, катфишинга, когда мошенник, вводя жертву в заблуждение, выманивает у нее крупную сумму денег.*

Abstract. *The consequences of identity theft in the social network, leading to the creation of fake profile are considered. Subsequently, these profiles are used for fraudulent contravene the romance scams, catfishing, when the fraudster (catfisher), introducing the victim to misleading entices her a large sum of money.*

Ключевые слова: *интернет-безопасность, персональные данные, кража идентичности, сетевое мошенничество, любовные аферы, катфишинг, аутентификация в социальной сети*

Keywords: *Internet safety, personal data, identity theft, network fraud, romance scam, catfishing, social network autentification*

Говоря о сегодняшних мобильных технологиях проникающих во все сферы нашей жизни, нельзя не отметить и те опасности, которые эти технологии могут привнести усилиями людей с преступными намерениями, способных использовать и наше стремление к комфорту, и нашу неосведомленность или доверчивость.

Поэтому перед преподавателями стоит задача, если не сказать, обязанность, не только повысить уровень собственной осведомленности, но и донести свои знания до учащихся, которые только начинают путешествие в этом высокотехнологичном мире, не задумываясь о потенциальных опасностях.

Кража идентичности стала самой растущей разновидностью преступлений в Соединенных Штатах. Например, в 2013 году каждые две минуты там совершалось преступление, связанное с кражей идентичности. В результате за год пострадало около 13 миллионов человек [1]. Мошенники используют украденную информацию по-разному (подделка банковских карт, кража медицинских страховок и т.д.).

О краже идентичности в социальных сетях с целью создания фальшивых аккаунтов говорилось в [2]. Упоминалась история профессора из Канады, фотоматериалы которого были использованы для знакомства с женщинами в мошеннических целях (по-английски этот вид мошенничества называется romantic scam или catfishing [3]. В русском языке используется транслитерация последнего – катфишинг, а мошенники – это катфишеры). Предлагаемый материал в определенной степени является развитием [2] и представляет собой описание последовательности действий с целью проверки, является ли новый сетевой знакомый тем, за кого себя выдает. Материал может быть полезен как для личного использования, так и в качестве учебного материала.

Шаг 1: Самое простое действие, с которого можно начать – это оценка подлинности фотографии, представленной в профиле нового знакомого. Следует пропустить изображение через обратный поиск изображений Google и посмотреть, где еще изображение появится. Для обратного поиска изображений можно также использовать сайт TinEye. Если изображение связано с разными именами или профилями, вполне вероятно, что аккаунт -мошеннический.

Шаг 2: Критический анализ био (краткая информация о владельце аккаунта). Катфишинговые аккаунты часто используют специфические биографические компоненты. Некоторые аспекты, которые должны вызвать настороженность:

- Статус «овдовел» или «разведена». Очевидно, что не все овдовевшие или разведенные люди – катфишеры, но этот статус в сочетании с другими особенностями может быть признаком фальшивого аккаунта.
- Работа, которая имеет исключительный статус, требующий постоянных поездок и / или периодов без связи (например, военный, инженер, нефтяник и т.д.), что помогает мошеннику оправдываться за то, что долгое время был не доступен для связи.

• Информация «О себе» содержит романтические клише, такие, например, как «ищет любовь» или заявления, которые могут стереотипно укрепить впечатление, например, «богобоязненный», наличие орфографических ошибок в названии предполагаемой «альма-матер.»

Шаг 3. Анализ имени тоже может послужить подсказкой относительно легитимности профиля:

• Многие мошенники, похоже, выбирают своё из списка популярных имен. Если поискать имя обладателя профиля на Facebook-е, и всплывёт множество других профилей с тем же именем и аналогичными профессиями, профиль следует изучить более внимательно.

• Можно «погуглить» имя профиля. У большинства людей есть по крайней мере какой-то цифровой след в эти дни. Можно ли найти человека? То, что удается найти, совпадает ли с тем, что говорится?

Шаг 4: Исследование профиля. Некоторые другие элементы профиля для анализа:

• Количество друзей: сколько у человека друзей? Взаимодействуют ли его друзья между собой?

• Типы друзей: Часто список друзей мошенника состоит, в подавляющем большинстве случаев, из людей противоположного пола.

• Возраст профиля: Профиль совершенно новый, или есть история загрузок фото, обновления статуса, сообщения от других, и т.д.? Кроме того, следует обратить внимание, что сообщения профиля можно пометить задним числом, чтобы создать впечатление, будто профиль имеет более длинную историю, чем на самом деле. Тем не менее, год создания профиля (Facebook) подделать невозможно..

• Наличие общих друзей. Следует отметить, что наличие небольшого числа общих друзей не обязательно является гарантией легитимности: мошенники иногда просятся в друзья друзей, чтобы сделать свой профиль более правдоподобным. Если общих друзей не много, то можно связаться с ними, чтобы выяснить, действительно ли они знают этого человека. Иногда бывает, что человека принимают в «друзья» на основа или фальшивого профиля, или просто по ошибке.

• Религиозная принадлежность: Мошенники также часто представляются, как очень религиозные люди и иногда используют писание или религиозный язык, чтобы казаться более надежным или манипулировать своими жертвами через общие системы верований.

Шаг 5: Наблюдение за поведением. Мошенники часто следуют предсказуемым моделям поведения, имеющим общие признаки, на которые следует обратить внимание:

• Быстрый перенос общения в личную переписку: электронная почта, смс или другой сервис мгновенного обмена сообщениями. Это делается для того, что если сеть идентифицирует исходный профиль как поддельный и удалит его из социальной сети, мошенник не теряет непосредственного контакта со своей потенциальной жертвой.

• Стремление к быстрому созданию обязательств: мошенники развивают онлайновые отношения очень быстро и зачастую могут заговорить о любви или о браке всего лишь через несколько дней общения; это способствует формированию у жертвы привязанности и чувства ответственности, что впоследствии поможет мошеннику обратиться к жертве за помощью;

• Отказ в использовании видеосвязи: мошенники зачастую предпочитают пользоваться только текстовой или голосовой связью, оправдывая отсутствие альтернативных возможностей, например, использования Skype, ненадежной связью. Если же все-таки сеанс связи состоится, изображение может быть очень низкого качества, а в артикуляции не совпадать со

звуком. Это будет объяснено плохой связью, а видео может быть скопировано из Youtube. По этой же причине может быть сокращена и продолжительность видео-общения.

• Мошенники нередко договариваются с жертвой о встрече, но эти планы никогда не реализуются по той или иной причине. В последний момент всегда возникает некоторое непреодолимое препятствие.

• Чрезвычайные ситуации: После того, как мошенник «зацепил» свою жертву, он приступает к отработке «чрезвычайной ситуации». Это может быть болезнь, потеря работы, необходимость по какой-либо причине срочной смены места пребывания и т.д.

• Просьба о деньгах: Это очевидный признак того, что новый знакомый – мошенник. Просьба может принимать различные формы, главное – обустроить перевод денег таким образом, чтобы в результате получателя невозможно было выявить, например, просьба об отправке денег через Western Union. Иногда жертву могут попросить перевести деньги «третьему лицу».

Шаг 6: Запрос на подтверждение идентификации. Если все же остаются некоторые сомнения, что человек на той стороне провода – мошенник, можно прибегнуть к той или иной форме подтверждения..

• Паспорт: в качестве документа, удостоверяющего личность, мошенник может предоставить паспорт, изготовленный с помощью фотошопа. Если паспорт покажется сомнительным, можно поискать в интернете, как выглядят реальные паспорта из разных стран. Сравнить, например, насколько фото на паспорте соответствует требованиям страны: размер / форма.

• В случае, если все же удастся организовать видео-общение в режиме реального времени можно попросить своего «знакомого» выполнить определенные действия, например, показать газету с датой того дня, хлопнуть в ладоши и т.д.

И главное, о чем не следует забывать – это здравый смысл. Если профиль выглядит чрезвычайно привлекательным, слишком хорошим, чтобы быть правдой, то весьма вероятно что действует профессиональный мошенник.

Что делать, если все же возникла уверенность, что это мошенник?

Шаг 7. После того, как возникла уверенность, что общение происходит с катфишером, следует предпринять несколько шагов.

• Проинформировать службу социальной сети.

• Исключить катфишера из списка друзей.

• Предупредить своих друзей.

Разговор о краже идентичности вывел на другую проблему, когда жертвами становятся не только обманутые люди, но и те, чьими данными мошенники пользуются для создания ложных профилей в социальных сетях. Поэтому, размещая свои фотографии на своих страницах, следует хорошо подумать, так ли необходимо их размещать. А размещаемые фото снабжать «водяными знаками»(water marks), отмечающими принадлежность фотографии [4] .

Список литературы

1. *Shin, L.* Someone had taken over my life: an identity theft victim's story / L. Shin [Электронный ресурс] // Forbes, 2014. November, 18. Режим доступа: http://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/#1b40bcce9787 (Дата обращения: 03.02.2017).

2. *Богданова, Д. А.* Еще раз о социальных медиа или обратная сторона медали / Д. А. Богданова // Материалы IX международной научно-практической конференции Новые информационные технологии в образовании 15-18 марта 2016 г. Екатеринбург. С. 130-132

3. Hielderbrant, K. Portfolio and research / K. Hielderbrant [Электронный ресурс] // Katia-Hielderbrant, 2016. June, 30 [Режим доступа: http://katiahielderbrant.ca/are-you-being-catfished/ (Дата обращения: 03.02.2017).

4. *Богданова Д.А.* По обе стороны экрана / Д. А. Богданова, А. А. Федосеев // Дистанционное и виртуальное обучение. 2015. №6. С. 87-96

УДК 378.147.1:004.738

А. И. Вагина, К. А. Федулова

К ВОПРОСУ О ИСПОЛЬЗОВАНИИ WEB 2.0 ТЕХНОЛОГИИ В ПРОЦЕССЕ ОБУЧЕНИЯ

Вагина Анастасия Игоревна
Федулова Ксения Анатольевна
vagina.nastya2013@yandex.ru
ФГАОУ ВО «Российский государственный профессионально-педагогический университет», Россия, г. Екатеринбург

THE QUESTION OF THE USING OF WEB 2.0 TECHNOLOGIES IN TEACHING

Vagina Anastasia Igorevna
Fedulova Ksenia Anatolievna
Russian State Vocational Pedagogical University, Russia, Yekaterinburg

Аннотация. *В статье рассматриваются вопросы применения современных сетевых ресурсов для повышения качества подготовки бакалавров при организации самостоятельной работы студентов.*

Abstract. *The author of the article discusses the using of modern network resources to improve the quality of training of bachelors in the organization of independent work of students.*

Ключевые слова: *сетевые сервисы, технологии Web 2.0, качество подготовки бакалавров, информационные технологии, дистанционное обучение.*

Keywords: *network services, Web 2.0 technologies, quality of preparation of bachelor, information technology, distance learning.*

Образование является одной из важнейших сфер человеческой деятельности, обеспечивающей формирование интеллектуального потенциала общества. Сложное положение образования России в настоящее время определяется рядом проблем, среди которых противоречие между традиционным темпом обучения и постоянно увеличивающейся скоростью появления новых знаний. Современные стандарты образования нацелены на увеличение количества и качества самостоятельной работы студентов, а для ее правильной организации необходимо вовремя и в достаточно большом объеме размещать информационные, методические и технические материалы, а порой и программные ресурсы.