www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.2.4

УДК 004.4
ББК 30.1

ИНТЕРНЕТ-МОШЕННИЧЕСТВО КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Мария Александровна Маслова

Аспирант, старший преподаватель
кафедры информационной безопасности,
Севастопольский государственный университет
ryzhaya.kristina@inbox.ru
ул. Университетская, 33, 299001 г. Севастополь, Российская Федерация

Кристина Юрьевна Рыжая

Студентка кафедры информационной безопасности,
Севастопольский государственный университет
ryzhaya.kristina@inbox.ru
ул. Университетская, 33, 299001 г. Севастополь, Российская Федерация

Аннотация. В данной статье будут рассмотрены основные виды и схемы интернет-мошенничества, новые угрозы для пользователя интернетом, а также рекомендации и программные методы по защите пользователей от таких угроз.

Ключевые слова: интернет-мошенничество, угроза, фишинг, биометрия, информационная безопасность, цифровой отпечаток.

Постановка проблемы. В век цифровых технологий перед пользователями интернета раскрывается множество возможностей, вспомогательных сайтов и приложений, как для работы, так и оплаты товаров и услуг. Большинство пользователей сети Интернет усвоили основные азы информационной безопасности: сегодня уже не каждый будет переходить по подозрительным ссылкам из писем или SMS-сообщений, но и интернет-мошенники, понимая это, придумывают все новые способы обмана.

Цель статьи – проанализировать статистику реализации известных информационных угроз, рассмотреть новые виды интернет-мошенничества и выработать рекомендации по защите от несанкционированных действий интернет-мошенников.

Интернет-мошенничество уже давно вышло за рамки почтовой рассылки и приобрело большие масштабы. Мошенники действуют практически во всех сферах человеческой деятельности, а с приходом в жизнь различных средств коммуникаций их деятельность приобрела новые тенденции.

Самые распространенные методы интернет-мошенничества: поддельные магазины с продажей через интернет, фишинг, сборы средств для благотворительности, сайты знакомств, вирусный контент.

Большим спросом пользуются продажи через интернет. Такое мошенничество осуще-

ствляется через поддельные магазины, магазины «однодневки», магазины, созданные на страничках пользователей в социальных сетях. После совершения покупки такие магазины исчезают, либо товар координально отличается от заявленного.

Фишинговые атаки все еще остаются актуальными. Доказательство тому – статистика «Лаборатории Касперского». В 2018 году на компьютерах пользователей продуктов «Лаборатории Касперского» было зафиксировано 482 465 211 срабатываний системы «Антифишинг» при попытках перехода на фишинговые сайты – это на 236 233 566 больше, чем в 2017 году. Всего было атаковано 18,32 % пользователей продуктов «Лаборатории Касперкого» [5].

У фишеров появились и новые цели. По данным «Лаборатории Касперского» за 2018 год были зафиксированы фишинговые атаки на 131 университет в 16 странах мира. Больше половины из них 83 высших учебных заведения – находятся в США, 21 – в Великобритании, по 7 в Австралии и Канаде. Одним из результатов деятельности мошенников стало похищение большого количества документов (в том числе исследований в области атомной энергетики) из нескольких университетов Великобритании [5].

Сборы средств для благотворительности являются очень популярными. Мошенники рассылают письма и SMS с просьбой о помощи, в которой зачастую нуждается ребенок или животное. Люди переводят деньги на счета, которые не являются благотворительными компаниями, в итоге денежные средства похищаются. Хотя и существует закон УК РФ по ст. 159.6 о мошенничестве в сфере компьютерной информации, но данное деяние очень трудно доказуемо, так как человек отдает деньги добровольно [1].

При создании поддельных сайтов или сообщений в социальных сетях злоумышленники редко изменяют свои реквизиты, поэтому скопировав платежные реквизиты в любой поисковик, можно проверить, нет ли предупреждений о мошенничестве.

Сайты знакомств всегда привлекали, и будут привлекать население любого возраста. Очень часто под заявляемым человеком на сайте, находится совершенно другой. Входя в доверие человек просит у другой стороны денежные средства на какие-либо нужды, оплату долгов или операцию, срочную покупку или на приезд в гости к нему. Но потом пропадает [2, с. 126].

Вирусный контент. Для создания вирусного контента злоумышленники используют все, что наиболее интересно пользователям. В последнее время популярны сериалы, поэтому злоумышленники часто используют их для своих целей. Исследователи из «Лаборатории Касперского» отобрали 31 сериал и выяснили, что самым популярным среди мошенников оказался сериал «Игра Престолов». Согласно статистике, связанных с «Игрой Престолов» программ, наносящих вред компьютеру, которые атаковали пользователей в 2018 году насчитывается 9 986 [4].

Один из новых методов мошенничества – это «фэйковые» приложения. Чаще всего «фейк» выдает себя за популярные мессенджеры и приложения или даже за игру.

Приложение «ANCESTRY LOOKUP» – это яркий тому пример. Данное приложение помогает пользователю найти своих предков. Для этого необходимо ввести свои фамилию, имя и отчество, дату и место рождения. Когда же пользователь приложит палец к сканнеру отпечатка, то он окажется подписан на платную версию приложения. Пользователь даже не будет подозревать, что с его счета списывается плата.

Такими приложениями могут быть различные прогнозы погоды, QR-считыватели и другие программы, характерной чертой которых является их незначительный или даже минимальный функционал. И проблема такого мошенничества заключается в том, что большинство пользователей – не читает пользовательское соглашение.

Личные данные пользователей – еще одна цель интернет-мошенников. Так, например, результатом работы приложения «GetContact» стали миллионы украденных и распространенных телефонных номеров с именами. И это не учитывая то, что некоторые пользователи записывают в контакты номера банковских карт, PIN-кодов и паролей от личных кабинетов, что является кладезем для мошенников.

Чтобы защититься от таких видов мошенничества, необходимо читать пользовательские соглашения, не скачивать незнакомые приложения с маленьким функционалом. Кроме того, необходимо настроить не только свой телефон так, чтоб приходили уведомления обо всех попытках списать со счета деньги за любое приложение, но и позаботиться о своих близких и знакомых, которые не умеют этого делать самостоятельно.

Использование «цифрового двойника» – это новый вид мошенничества, который связан с банковской сферой. В даркнете существует рынок под названием «Genesis», где продаются цифровые маски, которые включают в себя историю посещения сайтов, информацию об операционной системе, браузере, установленных плагинах и так далее.

Цифровой отпечаток – это то, что используют современные системы защиты от мошенничества для проверки подлинности пользователя. Если защитное решение видит маску, которая совпадает с той, что пользователь применял ранее, то транзакция будет одобрена. Многие банки в этом случае не станут отправлять код безопасности по SMS или уведомление для подтверждения операции [3].

Таким образом, при наличии цифровой маски и учетных данных пользователя в системе онлайн-банкинга, система защиты может принять интернет-мошенника за легитимного пользователя и не станет предпринимать какие-либо меры. Именно по этой причине мошенники собирают все возможные данные с устройств, а затем продают их на «Genesis». Покупая эти данные, злоумышленники выдают себя за владельцев цифровой маски.

Основная проблема такого мошенничества заключается в том, что банковские системы защиты от мошенничества используют те же данные, которые собирают злоумышленники. Чтобы защититься от такого вида краж денег с карты, банкам необходимо использовать двухфакторную аутентификацию. Можно предположить, что эффективным будет в качестве второго фактора использовать проверку биометрических данных: отпечатка пальца, сканирование радужной оболочки глаза, распознавание по геометрии лица. Так же важным этапом по улучшению безопасности будет информирование банков о всех новых актуальных видах и схемах мошенничества с целью принятия своевременных и предупредительных мер по предотвращению мошенничества.

Выводы. Рассмотренные методы интернет-мошенничества связаны не столько с интернетом, сколько непосредственно с пользователем. Пользователи сети Интернет должны не только знать о возможных видах и схемах мошенничества, а также позаботиться о программных методах защиты, таких как антивирус и своевременное обновление всех приложений, браузеров и систем. Только идя со временем, постоянно обучаясь и интересуясь как новыми угрозами, так и методами защиты от них – пользователь может обезопасить себя и своих близких от потерь.

СПИСОК ЛИТЕРАТУРЫ

1. Демидова, А. С. Мошенничество в сети интернет, как угроза экономической безопасности молодежи / А. С. Демидова, А. А. Поляруш. – Екатеринбург : УрФУ, 2017. – Электрон. текстовые дан. – Режим доступа: https: //cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kak-ugroza-ekonomicheskoy-bezopasnosti-molodezhi. – Загл. с экрана.

2. Интернет-мошенничество. Старые и новые угрозы / Е. А. Заплатина, Ю. В. Калинина, Е. А. Еремина, Д. В. Лопатин // Психолого-педагогичский журнал Гаудеамус, 2012. – № 2 (20). – С. 125–127.

3. Как жулики используют цифрового двойника, чтобы расплатиться вашей картой. – Электрон. текстовые дан. – Режим доступа: https://www.kaspersky.ru/blog/digital-masks-card-fraud/22584/. – Загл. с экрана.

4. Об опасности популярных сериалов. – Электрон. текстовые дан. – Режим доступа: https://www.kaspersky.ru/blog/tv-series-threats/22542/. – Загл. с экрана.

5. Спам и фишинг в 2018 году. – Электрон. текстовые дан. – Режим доступа: https://securelist.ru/spam-and-phishing-in-2018/93453. – Загл. с экрана.

REFERENCES

1. Demidova A.S., Polyarush A.A. *Moshennichestvo v seti internet, kak ugroza ekonomicheskoy bezopasnosti molodezhi* [Fraud on the Internet as a Threat to Economic Security of Young

People]. Yekaterinburg, UrFU, 2017. URL: https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kak-ugroza-ekonomicheskoy-bezopasnosti-molodezhi.

2. Zaplatina E.A., Kalinina Yu.V., Eremina E.A., Lopatin D.V. Internet-moshennichestvo. Starye i novye ugrozy [Internet Fraud. Old and New Threats]. *Psikhologo-pedagogichskiy zhurnal Gaudeamus* [Psychological-Pedagogical Journal GAUDEAMUS], no. 2 (20), 2012, pp.125-127.

3. *Kak zhuliki ispolzuyut tsifrovogo dvoynika, chtoby rasplatitsya vashey kartoy* [How Fraudsters Use a Digital Twin to Pay with Your Card.]. URL: https://www.kaspersky.ru/blog/digital-masks-card-fraud/22584.

4. *Ob opasnosti populyarnykh serialov* [On the Dangers of Popular TV Series]. URL: https://www.kaspersky.ru/blog/tv-series-threats/22542.

5. *Spam i fishing v 2018 godu* [Spam and Phishing in 2018.]. URL: https://securelist.ru/spam-and-phishing-in-2018/93453.

INTERNET FRAUD AS A THREAT TO PERSONAL INFORMATION SECURITY

Marija A. Maslova

Postgraduate Student, Senior Lecturer,
Department of Information Security,
Sevastopol State University
ryzhaya.kristina@inbox.ru
Universitetskaya St., 33, 299001 Sevastopol, Russian Federation

Kristina Ju. Ryzhaja

Student, Department of Information Security,
Sevastopol State University
ryzhaya.kristina@inbox.ru
Universitetskaya St., 33, 299001 Sevastopol, Russian Federation

Abstract. The paper analyzes the statistics of implementing known information threats, considers new types of Internet fraud and develops recommendations for protecting against unauthorized actions of Internet scammers.

Internet fraud has long gone beyond mailing and has become widespread. Fraudsters operate in almost all spheres of human activity, and with the advent of various means of communication their activities have acquired new trends.

The most common methods of online fraud are the following: fake shops with Internet sales, phishing, fundraising for charity, dating sites, viral content.

The paper shows that the considered methods of Internet fraud are connected not so much with the Internet as directly with the user. Internet users should not only be aware of possible types and schemes of fraud, but also take care of software protection methods such as antivirus and timely updating all applications, browsers and systems. Only being up to date, constantly learning and being interested in both new threats and methods of their protection users can protect themselves and their loved ones from losses.

Key words: Internet-fraud, threat, phishing, biometrics, information security, digital fingerprint.