В целях профилактики киберпреступлений

В связи с динамичным и масштабным ростом числа киберугроз и киберпреступлений, причиняемым ими ущербом государственным структурам, юридическим и физическим лицам, такие противоправные деяния представляют серьезнейшую проблему для общества, а борьба с ними является актуальной и стратегически важной задачей для правоохранительных органов. Разветвленные элементы инфраструктуры сети Интернет, мобильных сетей связи (телекоммуникации) являются наиболее востребованными средствами совершения преступлений, как для хакеров, так и для различного рода мошенников, террористов, торговцев людьми, порнографией, наркотиками, а также в целях совершения сексуального насилия и развратных действий в отношении несовершеннолетних (малолетних).

Следственным управлением Следственного комитета Российской Федерации по Ярославской области совместно с другими правоохранительными органами региона проводится постоянная целенаправленная работа по противодействию киберпреступности, в том числе совершаемой в банковской сфере в отношении граждан, производящих платежи посредством использования сети Интернет.

Действительная реальность такова, что сегодня техническими возможностями компьютеров, их программным обеспечением, сетью Интернет, сотовой связью стремятся воспользоваться криминальные элементы, количество которых с каждым днем возрастает, а расширяющаяся глобализация информационных процессов и пространства, способствует созданию новых способов, средств и объектов преступных киберпосягательств.

Злоумышленники все чаще стали использовать новые электронные способы и средства, например, мобильные системы связи, возможности интернет-банкинга.

Важную роль в вопросе противодействия незаконной деятельности киберпреступников является предусмотрительность и соблюдение элементарных правил производства электронных платежей самими гражданами, некоторыми из них могут быть:

- К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

- Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

- Храните номер карточки и ПИН–коды в тайне. Запомните и заклейте CVC-код.

- Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

- Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

- Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

- Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

- Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

- Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

- Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

- Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

Внимание! Информация Банка России

Злоумышленники готовятся к кибератакам под Новый год

Киберпреступность, ориентированная в первую очередь на хищение денег у кредитно-финансовых организаций и их клиентов, стала одной из главных угроз современного мира. Глобальный ущерб от нее уже превышает 1% мирового ВВП и продолжает быстро увеличиваться.

Финансовые организации объединяют усилия для борьбы с кибермошенниками. Банк России

выпустил ряд регламентирующих документов, в частности положение «О требованиях к защите информации в платежной системе Банка России», обязывающее банки в жесткие сроки сообщать о киберинцидентах. Создан и профессиональнодействует Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере (FinCERT), интеграция которого с коммерческими и банковскими центрами мониторинга должна способствовать уменьшению количества масштабных кибератак и снижению потерь от них. К информационному обмену о такого рода угрозах присоединились уже 95% организаций, которые представлены на отечественном финансовом рынке.

А в ближайшем будущем регулятор намерен выстроить единый фронт борьбы финансовых организаций с хакерами, ворующими деньги со счетов граждан и компаний. Кредитные организации будут обязаны внедрять системы, препятствующие незаконному списанию денег со счетов и их обналичиванию - так называемые системы антифрода. То есть банки при подозрении, что операция по переводу или снятию денег с карты осуществляется без ведома владельца денег, должны уточнить у него, действительно ли он совершает транзакцию. Банк также будет сам определять, какой конкретный механизм, какое программное средство ему подходят исходя из его масштабов, клиентской базы, технической оснащенности. Кроме того, предусматривается регламентировать обмен банков информацией о счетах так называемых дропперов - физических и юридических лиц, через которые проходят похищенные деньги. Это поможет противодействовать запуску в теневой оборот и обналичиванию украденных денег.

Проблемой озадачились и на государственном уровне. Так, российское правительство внесло в Госдуму законопроект, дающий право банкам блокировать карты и счета клиентов в том случае, если проводимые ими финансовые операции представляются кредитным организациям подозрительными. Базовые требования к антимошенническим системам остановки и возврата платежей – так предусматривает законопроект - установит Банк России. Законопроект об остановке и возврате мошеннических переводов денежных средств Госдума планирует рассмотреть в весеннюю сессию.

Человек сам кузнец своего счастья. И очень часто – несчастья тоже. Преступность свести к нулю невозможно, но нам нужно создать условия, в которых злоумышленникам в России было бы некомфортно. Это не только задача Банка России, это задача и финансовых организаций, и правоохранительных органов. Злоумышленники традиционно готовятся к кибератакам под Новый год.

Кстати, это мировая тенденция. Согласно прогнозам банка Barclays, убытки покупателей от предпраздничного кибермошенничества в Великобритании в декабре 2017 года могут превысить 1,3 млрд фунтов. Поэтому, покупая подарки, обновки и разносолы к новогоднему столу, будьте бдительны. Эксперты рекомендуют проверять наличие символа замка и аббревиатуры «https» в адресной строке на веб-сайтах розничной торговли, никогда не использовать публичный Wi-Fi для осуществления транзакций, никогда и никому не раскрывать уникальные данные своей карты 9 в том числе уникальные коды для

подтверждения транзакций, которые банк присылает вам в SMS) и персональные данные, а также не лениться и регулярно проверять остаток на своем счете.

Памятка Банка России

В интернете активизировались финансовые мошенники

Деятельность более 400 нелегальных доменных имен, связанных с финансовым мошенничеством, кражей личной информации и распространением вирусов, прекращена по инициативе Банка России. Организации, стоявшие за ними, занимались различными видами финансового мошенничества в интернете. Жулики маскировались под микрофинансовые организации, банки, форекс-дилеров, страховые компании. Однако никакого права работать в этой сфере они не имели.

Как уберечь свои кровно заработанные деньги от современных «интернет-продвинутых» котов Базилио и лисиц Алис?

Все легально действующие игроки на финансовом рынке обязаны иметь лицензию Банка России. Для потребителя подобная лицензия – это гарантия защиты его прав.

«Проверить наличие лицензии не сложно, достаточно зайти на сайт www.cbr.ru в раздел «Финансовые рынки», где представлен «Справочник участников финансового рынка»».На этом же сайте опубликованы постоянно обновляющиеся государственные реестры микрофинансовых организаций и кредитных потребительских кооперативов.

Ищите «белую метку»

Как же сегодня мошенники в интернете обманывают своих жертв? В основном, пользуясь невнимательностью граждан или их стремлением заработать легкие деньги. Одним из самых распространенных способов обмана можно считать **махинации «черных» кредиторов.** Эти жулики действуют разными методами. К примеру, организуют рассылку одобрений на «кредит» или звонят по телефону, рассчитывая, что хоть кто-то из адресатов действительно подавал подобную заявку. Откликнувшейся на предложение жертве предлагается заплатить «комиссию» за одобрение или рассмотрение заявки, причем, сделать перевод через крупный

банк. Кстати, когда клиенты начинают жаловаться, что не получили кредит, самые циничные аферисты предлагают им… заплатить за рассмотрение «заявки» еще раз.

Впрочем, человек и сам может наткнуться на нелегальных кредиторов, когда ищет в интернете, где бы занять или куда под наибольший процент вложить деньги. В этом случае мошенники расставляют ловушку следующим образом: создают сайт, как две капли воды похожий на интернет-представительство известной финансовой компании. Человек без колебаний заполняет заявку на кредит, порой раскрывая данные своей банковской карты, – а в конце онлайн-цепочки остается и беззаемных, и без собственных денег.

Иногда финансовые организации, которые лишились лицензии, продолжают через интернет предлагать «заем до зарплаты». Такая деятельность также незаконна. Чтобы клиенту было проще опознать мошенников, Банк России применяет схему, разработанную вместе с Яндексом. В результатах поиска микрофинансовые организации обозначаются специальным знаком «Реестр ЦБ РФ».

Выявляет Банк России также случаи, когда финансовые мошенники сумели обмануть не отдельных граждан, а целые предприятия. К примеру,организации с автопарком аферисты сумели продать поддельные полисы каско.

Пирамиды маскируются

В интернете прочно обосновались финансовые пирамиды –компании, выплачивающие деньги вкладчикам из средств вновь пришедших клиентов. Мониторинг Международной конфедерации обществ потребителей (КонфОП) показал, что подобные компании занимают верхние позиции в топ-30 поисковых запросов в интернете по вложениям средств.Организаторы мониторинга изучили выдачу поисковых систем «Яндекс» и Google по запросу «вложить деньги выгодно» с настройками, обеспечивающими объективность выборки, и затем провели анализ сайтов небанковских организаций, предлагающих вложение средств. Среди наиболее характерных признаков 25 выбранных организаций – обещания супердоходности, рассказы об «уникальных продуктах» и неправомерное использование символов государственной власти.

Мошенники могут называть себя инвестиционными фондами, прикрываться известными названиями и убеждать, что деньги вкладываются в «высокодоходные проекты». Например, представленные в мониторинге КонфОП компании обещали клиентам различный уровень доходности – от умеренной в 10–12% (за инвестиции в солнечную энергетику в Испании) до практически неосуществимой в 550% («игра» в ценные бумаги). Половина из рассмотренных компаний решили не указывать на сайте свои реквизиты, но при этом разместили различные «свидетельства» и «сертификаты» (в том числе иностранного происхождения),призванные

доказать их надежность и состоятельность.

Как отмечают в Банке России, перенос деятельности финансовых пирамид в интернет – это тенденция последнего времени.Сейчас на долю интернет-проектов приходится четверть выявленных пирамид, 46% приходится на фирмы с признаками фиктивности, 29% – это пирамиды, маскирующиеся под микрофинансовые организации и кредитно-потребительские кооперативы.

Спешить медленно

Собственно, для выявления мошенников Банк России использует систему автоматизированного мониторинга интернета. Но каждый из нас может помочь регулятору в борьбе с нечистыми на руку дельцами. «Если вы получили смс-сообщение, письмо или звонок от предполагаемых мошенников – напишите обращение в Банк России в интернет-приемной на сайте www.cbr.ru. Если пострадали от действий жуликов – обратитесь в правоохранительные органы.

А еще лучше – не попадать в подобные неприятные ситуации. Для этого нужно обязательно проверять лицензию финансовой организации, не верить излишне щедрым обещаниям и не спешить с принятием решений, связанных с деньгами.

Адрес страницы: https://yaroslavl.sledcom.ru/references/Ugolok-finansovoj-gramotnosti/item/1165543