**Будьте бдительны: предновогоднее кибермошенничество**

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 профессионально действует 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. Как недавно сообщил недавно заместитель начальника Главного управления безопасности и защиты информации Банка России Артем Сычев, 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, - рассказал Артем Сычев (цитата по интервью в «Российской газете» от 6 декабря 2017 года). - 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. «Мы понимаем, что 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», - отмечает Артем Сычев. И предупреждает всех нас: 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.

Для того чтобы обезопасить себя в эти предновогодние дни и не только, необходимо придерживаться следующих правил. Всегда проверяйте наличие символа замка и аббревиатуры «https» в адресной строке на веб-сайтах розничной торговли. Кроме

того, никогда не используйте публичный Wi-Fi для осуществления транзакций. Ни в коем случае не реагируйте на электронные сообщения, в которых вас просят предоставить реквизиты счета, PIN-коды, пароли или персональные данные. Всегда используйте надежные уникальные пароли для максимально возможного количества учетных записей в интернете, а лучше всего – индивидуальный пароль для каждой из них. Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для «автоматического заполнения» при открытии интернет-сайта или приложения.