О противодействии финансовому мошенничеству

Как защитить себя от интернет-мошенников

По официальным данным МВД РФ, за январь-февраль 2021 года зарегистрировано на 29,4% больше IT-преступлений, чем год назад, в том числе совершенных с использованием сети «Интернет» – на 48,3% и при помощи средств мобильной связи – на 32,6%. Если в январе-феврале 2020 года удельный вес преступлений в IT-сфере составлял 19,3%, то за первые 2 месяца текущего года он увеличился до 26,3%.

Эксперты выявили рост финансовых потерь россиян от действий интернет-мошенников. Ущерб от их деятельности оценивается в миллиарды рублей.

Связывают это, в частности, с тем, что россияне стали активно пользоваться различными онлайн-услугами, а также чаще покупать товары в интернет-магазинах.

В Интернете существует множество сайтов, где любой желающий может оставить свой отзыв или вопрос.

Однако, стоит понимать, что некоторые сайты, являются «фейковыми» и разработаны специально для того, чтобы осуществлять сбор информации и отслеживание персональных данных, но основная их цель - наши с вами кошельки.

Получая информацию о нас, как о потребителях тех или иных услуг, они анализируют наше поведение, потребительский менталитет, покупательные способности, начиная с того, что мы покупаем, сколько, где и т.д., с целью скрытной передачи сведений торговым сервисам и другим заинтересованным лицам, в том числе, криминальным элементам.

Для кражи денежных средств интернет-мошенники используют сайты-приманки, на которые выставляют товары повышенного спроса по низкой цене. Происходит это следующим образом. В том случае, когда Покупатель принимает решение о покупке, специальная форма обратной связи переводит его по ссылке на вредоносный ресурс, где специальная программа крадёт данные о банковской карте. В результате чего, гражданин лишается товара и денежных средств.

Надо понимать, что современные хакеры — это уже не те студенты и школьники из 90-х, которые ради интереса, «взламывают» сети министерств и ведомств, сегодняшний «хакер» может выглядеть как преуспевающий бизнесмен, окончивший престижный технический вуз.

Превентивные меры

Предупрежден – значит, вооружен.

Изучив различные схемы интернет-мошенничества, можно дать несколько рекомендаций.

Во-первых, к защите информации своих персональных данных и имущества, нужно относится, более чем серьезно и основательно, поскольку злоумышленники «взломав» информацию на компьютере, могут вывести его из строя, внедрив в него «вирус».

Поэтому, на компьютере, прежде всего, нужно установить защиту от возможных хакерских атак.

Например, Avast, Kaspersky и другие условно бесплатные антивирусные программы.

Во-вторых, не использовать подозрительные сайты, мобильные приложения, а использовать информацию из первоисточников, а именно, сайты официальных министерств и ведомств.

В-третьих, чтобы избежать ситуации с кражей персональных данных, периодически необходимо производить полную очистку компьютера и удалять лишние программы и приложения, особенно те, которые не используются более месяца.

Про ответственность

Согласно ст. 17 ФЗ «Об информации, информационных технологиях и о защите информации», за нарушение требований о защите информации, предусмотрена дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством Российской Федерации.

В соответствии с п. 1 ст. 13.11 Кодекс Российской Федерации об административных правонарушениях, обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, влечет наложение административного штрафа на граждан в размере **от шести тысяч до десяти тысяч рублей**; на должностных лиц - **от двадцати тысяч до сорока тысяч рублей**; на юридических лиц - **от тридцати тысяч до ста пятидесяти тысяч рублей**.

Кроме того, для защиты граждан от телефонных мошенников принят Федеральный закон от 09.03.2021 № 44-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы", который позволит ликвидировать нелегальные «колл-центры», организованные на территории исправительных учреждений и изоляторов, жертвами которых часто становятся особо незащищенные слои населения, несовершеннолетние и пожилые люди.

Данный закон позволит осуществлять блокировку таких мобильных номеров и пресекать случаи телефонного мошенничества, кода людям, якобы “звонят из службы безопасности банка”.

Информация подготовлена специалистами
Консультационного центра по защите прав потребителей
ФБУЗ «Центр гигиены и эпидемиологии в Иркутской области»
с использованием материалов с сайта мвд.рф
и справочной системы Консультант плюс
Контактные данные:
г.Иркутск, ул.Трилиссера, 51, тел.8(395-2)22-23-88
ул. Пушкина, 8, тел. 8(395-2)63-66-22
*Email- **zpp@sesoirk.irkutsk.ru.***