О необходимости повышения уровня правовой и финансовой грамотности граждан и «компьютерной гигиене» физических и юридических лиц

В современном мире противодействие киберпреступности является одной из наиболее актуальных и сложных криминологических проблем. Высокая латентность, рост числа киберпреступников, совершенствование информационных технологий, создающие новые возможности совершения этих преступлений, необходимость иных подходов противодействия преступлениям, совершаемым в виртуальном пространстве, создают угрозы для глобальных информационных сетей и общества в целом.

Киберпреступления — это преступления, совершаемые с использованием современных информационно-коммуникационных технологий, т.е. с использованием компьютерной техники и/или Интернета в информационном (виртуальном) пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях, находящиеся в движении по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, или другого носителя, предназначенного для их хранения, обработки и передачи.

Преступления в данной сфере в настоящее время достигли определенного размаха, чему способствует повсеместное подключение к Интернету с помощью ноутбуков, смартфонов и планшетов, и по праву считается одной из самых прибыльных статей криминального бизнеса в целом. С помощью сети «Интернет» киберпреступники могут совершать преступление анонимно, скрывать свою истинную личность. Ее трансграничный характер не ограничивает преступников территориальным пространством и позволяет уходить от уголовной ответственности.

Наиболее часто киберпреступления являются финансово-ориентированными и осуществляются посредством следующие типов атак:

- **фишинг** - получение доступа к конфиденциальным данным пользователя (логинам и паролям), с помощью вирусов, шпионских программ, программ-вымогателей и другой социальной инженерии — чаще всего с целью кражи личных данных или финансовых средств.

В подобных схемах излюбленным средством злоумышленников является электронная почта. Суть метода заключается в принуждении получателя письма к переходу по ссылке от имени

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Тыва

легитимной организации (банка, налоговой службы, популярного интернет магазина и т. д.). В подобных случаях целью, зачастую, является овладение банковскими данными

- кибервымогательство. Как правило, у пользователя или компании после загрузки вредоносного кода шифруются файлы, а затем поступает предложение о восстановлении в обмен на денежное вознаграждение (обычно в виде биткоинов или другой криптовалюты), так как государственные денежные знаки можно отследить, а криптовалюту отследить сложно

- финансовое мошенничество, которое в основном связано со взломом компьютерных систем операторов розничной торговли с целью получения банковских данных о покупателях (так называемые целевые атаки) или последующими манипуляциями полученной информацией. Некоторые типы мошенничества, связанного с финансами, чрезвычайно сложно обнаружить.

Киберпреступники используют целый арсенал узкоспециальных знаний и навыков в целях получения несанкционированного доступа к банковским счетам, совершения краж личности, вымогательства финансовых средств, мошенничества, преследования и запугивания или использования зараженного компьютера в разветвленной сети с целью совершения атак на крупные организации.

Противодействие киберпреступлениям входит в обязанности правоохранительных органов. Но сами пользователи также могут существенно способствовать пресечению роста киберпреступности, заблокировав основной метод распространения киберпреступлений: вредоносное программное обеспечение.

Избавившись от вирусов, шпионского программного обеспечения и программ-вымогателей с помощью современного и эффективного антивируса Вы не только защитите свой компьютер от вредоносной программы, но пресечете попытки злоумышленников получать выгоду, в том числе Ваши финансовые средства противозаконно — что является их основной мотивацией.

Советы по предупреждению киберпреступлений:

- используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;

- установите антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и другую технику;

- не загружайте файлы из непроверенных источников;

- не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Тыва

- не сообщайте никому свои пароли и личные данные;

- воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги;

- используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов;

- воздержитесь от паролей – дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Соблюдение правил безопасной работы в Интернете, таких как воздержание от загрузок из неизвестных источников и посещения сайтов с низкой репутацией — это здравый смысл. Внимательное и бережное отношение к своим учетным и персональным данным может поспособствовать защите от киберзлоумышленников. Однако наиболее эффективным методом защиты по-прежнему остается использование современного и качественного антивирусного решения.

Адрес страницы: https://tuva.sledcom.ru/Pomoshh_detjam/item/1574670

© 2024 Следственное управление Следственного комитета Российской Федерации по Республике Тыва