



Рекомендации по повышению уровня правовой и финансовой грамотности граждан и «компьютерной гигиене» среди физических и юридических лиц

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, находящихся 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.

В современных условиях преступления в данной сфере достигли беспрецедентного размаха, чему чрезвычайно поспособствовало повсеместное подключение к Интернету с помощью ноутбуков, смартфонов и планшетов. С помощью сети Интернет киберпреступники могут совершать преступление анонимно, скрывая свою истинную личность. Кроме того, сфера деятельности преступников не ограничивается территориальным пространством.

Наиболее часто киберпреступления являются финансово-ориентированными и осуществляются посредством следующих 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 легитимной организации (банка, налоговой службы, популярного интернет магазина и т.д.). В подобных случаях целью, зачастую, является овладение банковскими данными.

- **кибервымогательство**

Как правило, вначале 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

Большинство изощренных схем финансового мошенничества 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, вымогательства финансовых средств, мошенничества, преследования и запугивания или использования зараженного компьютера в разветвленной сети с целью совершения атак на крупные организации.

Противодействие киберпреступлениям осуществляется правоохранительными органами. Пользователи также могут существенно поспособствовать пресечению роста киберпреступности, заблокировав 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 попытку злоумышленников получить выгоду.

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;
- 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



Официальный сайт

Следственное управление
Следственного комитета Российской Федерации
по Республике Коми

вычислить либо подобрать.

Обеспечение защиты от киберпреступлений может занять довольно продолжительное время и некоторых усилий по изучению различных правил поведения в киберпространстве, но всегда того стоит. Соблюдение таких правил безопасной работы в Интернете, как воздержание от загрузок из неизвестных источников и посещения сайтов с низкой репутацией — это здравый смысл в рамках предотвращения киберпреступлений. Внимательное и бережное отношение к своим учетным и персональным данным может поспособствовать защите от злоумышленников. Однако наиболее эффективным методом защиты по-прежнему остается использование современного и качественного антивирусного решения.

Адрес страницы: <https://komi.sledcom.ru/Pamyatki/item/1695349>