# Следственное управление напоминает правила "компьютерной гигиены"

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, то есть 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 беспрецедентного размаха, чему чрезвычайно поспособствовали всеобщая дигитализация и повсеместное подключение к Интернету с помощью ноутбуков, смартфонов и планшетов, и по праву считается одной из самых прибыльных статей криминального бизнеса в целом.

Пожалуй, главной причиной роста компьютерной преступности становятся ее криминогенные факторы, возникшие в ходе совершенствования сети Интернет. 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 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.

**Распространены киберпреступления, связанные со вторжением в частную жизнь.**

Существует несколько типов подобных киберпреступлений, целью которых является кража личной конфиденциальной информации. Хотя зачастую злоумышленниками движет более глубокая мотивация (например, денежная или связанная с изменением политических настроений), основное внимание сосредоточено на обходе законов и поиске брешей в технологиях, которые защищают персональные конфиденциальные сведения.

**- кража персональных данных.**

Кража личной информации обычно происходит с целью последующей подмены личности человека или группы людей. Хотя некоторые злоумышленники крадут паспорта или другие удостоверения личности для физической подмены личности, в основном кража персональных данных происходит исключительно в интернете.

Например, некто, желающий получить банковский заем, может украсть персональную информацию человека с хорошей кредитной историей.

**- шпионаж.**

Целью шпионажа, начиная от взломов индивидуальных компьютеров или устройств и заканчивая нелегальной массовой слежкой, является тайное отслеживание нашей частной жизни. Здесь может быть как физический шпионаж (например, при помощи веб- или CCTV-камер для наблюдения за отдельными персонами или группой людей), так и массовый мониторинг различного рода коммуникаций (чтение почты, текстовых сообщений мессенджеров, смс и так далее).

Также одной из распространенных форм киберпреступлений является **нарушение авторских прав**. В первую очередь в эту категорию попадает выкладка в общий доступ музыки, фотографий, фильмов, книг и т.д. без согласия авторов.

С использованием современных информационно-коммуникационных технологий совершаются преступления экстремистской и террористической направленности, преступления против половой неприкосновенности несовершеннолетних, кибербуллинг. И это далеко не весь перечень преступлений, которые можно отнести к категории киберпреступности.

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 с киберпреступлениями входит в обязанности правоохранительных органов.

Рядовые пользователи также могут существенно поспособствовать 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;

- 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.

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.

*18 Декабря 2022*

*Адрес страницы:* https://ryazan.sledcom.ru/news/item/1750922