**Люберецкая городская прокуратура разъясняет**

# **Противодействие преступности в сфере использования информационно-коммуникационных технологий**

В современном обществе одним из самых распространенных видов преступлений является мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием, в том числе совершенное дистанционным способом с использованием информационно-коммуникационных технологий. Данный вид мошенничества совершается как правило без физического контакта с потерпевшим.

Способы совершения хищения с использованием информационно-коммуникационных технологий постоянно совершенствуются, что создает определенные сложности для правоохранительных органов в раскрытии преступлений указанной категории.

Одним из самых распространенных видов хищения является телефонное мошенничество. Как правило, от имени сотрудников банков России, мошенники сообщают потерпевшему о несанкционированных списаниях денежных средств с банковских карт или сообщают о необходимой блокировки банковской карты. Далее, мошенники, войдя в доверие, просят предоставить определенные данные карты владельца или сообщить смс-код, поступивший на его телефон. В результате чего, как правило, происходит списание денежных средств с банковского счета.

Нужно помнить, что сотрудники банка при общении с клиентом банка никогда не просят сообщить ему реквизиты банковской карты. Зачастую мошенники могут представиться сотрудниками полиции и сообщают о том, что близкие родственники задержаны за совершение преступления либо стали виновниками дорожно-транспортного происшествия, в результате которого погибли люди. Для того, чтобы родственник избежал наказания мошенник предлагает заплатить определенную сумму денег. В последнее время участились случаи, когда за денежными средствами приезжают курьеры, либо мошенники просят перевести денежные средства через платежный терминал.

Также, довольно распространенным способом мошенничества на сегодняшний день является мошенничество в социальных сетях. В данном случае мошенники, с помощью взлома персональной страницы в социальных сетях, обращаются от лица потерпевшего с просьбой о помощи, а именно о переводе денежных средств на банковский счет, либо просят реквизиты карт, чтобы перевести деньги.

Мошенничество через «Интернет-магазин» - еще один способ обмана. Преступники берут с будущей жертвы предоплату или полную сумму за определенный товар, но не исполняют своих обязательств. Благодаря фальшивых интернет-сайтов, мошенники собирают реквизиты банковских карт потерпевших и далее используют для операций по обналичиванию денежных средств.

Будьте внимательны и осторожны при общении с посторонними лицами.

**Люберецкая городская прокуратура разъясняет**

# **Противодействии киберпреступности**

Киберпреступление – это преступления, совершенные в интернет пространстве, либо иной компьютерной сети с использованием информационно-компьютерных технологий, направленные на атаку компьютера, компьютерную сеть или сетевое устройство.

Киберпреступления совершаются в форме мошенничества, распространение вредоносных интернетссылок, установка на компьютер вредоносного программного обеспечения.

Когда информационно-компьютерные технологии являются частью совершения преступления, киберпреступление включает в себя как финансовую выгоду, так и получение другой ценной информации для киберпреступника, выведение из строя самого компьютера, либо сетевого устройства.

Законодательство Российской Федерации предусматривает различную ответственность за деяния подобного вида.

Так, за неправомерный доступ к компьютерной информации и другую ответственность за подобного рода деяния, если оно повлекло тяжкие последствия или создало угрозу их наступления предусмотрена уголовная ответственность по статье 272 Уголовного кодекса Российской Федерации, вплоть до лишения свободы на срок до 7 лет.

В случае создания, использования и распространения вредоносных компьютерных программ предусмотрена уголовная ответственность по статье 273 Уголовного кодекса Российской Федерации в виде принудительных работ либо лишением свободы на срок до семи лет.

В целях защиты от киберпреступлений физическим лицам следует использовать лицензионное программное обеспечение, антивируса на персональном компьютере, установление пароля. Кроме этого, не открывать разного рода ссылки и не переходить на сайт, если не уверены в его безопасности, а также не храните личную информацию в общедоступных ресурсах, таких как социальные сети, облачное хранилище и другое.

Также, существуют способы защиты от киберпреступности для юридических лиц, к ним относят:

- работа в специализированных программах через защищённое подключение;

- регистрация и учёт внешних носителей информации (флешнакопитель, съёмный жёсткий диск и т.п.);

- передача информации посредством рабочей электронной почты;

- отсутствие личной либо рабочей информации в общих папках формата «Облачное хранилище»;

- при наличии удалённой рабочей станции с рабочими файлами, использовать программный клиент для дальнейшего подключения к ней;

- использовать аппаратно-программный комплекс шифрования (АПКШ) для обеспечения защиты данных организации от вторжения со стороны сети-интернет.

**Люберецкая городская прокуратура разъясняет**

# **Преступления в сфере компьютерной информации**

В настоящее время с использованием информационно-телекоммуникационных сетей совершается множество видов преступлений, например распространение вирусного программного обеспечения; кража конфиденциальных данных пользователей; кража чужих продуктов интеллектуальной деятельности; взлом чужих аккаунтов в социальных сетях; распространение неверной информации, клевета; разжигание межнациональной розни или провокация межрелигиозной вражды, незаконный оборот наркотиков. Особенно распространенное преступление -мошенничество.

Киберпреступления сложнее раскрыть, поэтому за них предусмотрены более строгие санкции, чем за аналогичные действия, совершенные без использования информационных технологий.

В отдельную главу 28 Уголовного кодекса Российской Федерации выделены преступления в сфере компьютерной информации. Ответственность за данные преступления наступает с 16 лет.

Глава состоит из четырех статей.

Статья 272 УК РФ - неправомерный доступ к компьютерной информации. Подразумевает незаконное получение доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

За совершение подобных действий лицо может понести наказание в виде штрафа в размере до 200 тысяч рублей, исправительных работ - до года или лишения свободы до 2 лет.

Если эти деяния причинили крупный ущерб (свыше 1 миллиона рублей), либо были совершены из корыстной заинтересованности, группой лиц или лицом с использованием своего служебного положения, то размеры штрафов, сроки исправительных работ и лишения свободы увеличиваются.

В случаях, если вышеуказанные действия виновного лица повлекли тяжкие последствия или создали угрозу их наступления, то срок лишения свободы может быть определен в виде 7 лет. К тяжким последствиям относятся: причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого вреда здоровью людей или смерти и др.)

Статья 273 УК РФ - создание, использование и распространение вредоносных компьютерных программ. Предусматривает уголовную ответственность за создание, распространение или использование

компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирование компьютерной информации или нейтрализации средств защиты компьютерной информации.

Под компьютерными программами по смыслу данной статьи УК РФ в основном понимаются программы, известные как компьютерные вирусы,

За совершение указанных действий предусмотрено ограничение свободы или принудительные работы на срок до 4 лет, или лишение свободы до 4 лет со штрафом до 200 тысяч рублей.

Более суровые сроки наказания предусмотрены, за совершения этих действий группой лиц или лицом с использованием своего служебного положения, либо из корыстной заинтересованности, а также если они причинили крупный ущерб. А в случаях наступления тяжких последствий или создания угрозы их наступления срок лишения свободы может быть назначен виновному до 7 лет.

Статья 274 УК РФ - нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Согласно данной статье за некорректное использование компьютерной информации и информационно-телекоммуникационных сетей, вследствие которого повредилась охраняемая информация, была подвержена изменениям или скопирована, виновному грозит уголовная ответственность и наказание в виде штрафа до 500 тысяч рублей или исправительных работ сроком до 6 месяцев, или лишения свободы на срок до 2 лет.

Более суровое наказание - до 5 лет лишения свободы предусмотрев: если эти действия повлекли тяжкие последствия или создание угрозы их наступления.

Статья 274.1 УК РФ - неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Ответственность по данной статье наступает в случаях создания, распространения и (или) использование компьютерных программ, предназначенных для уничтожения, блокирования, модификации, копирования информации, содержащейся в критической информационной инфраструктуре Российской Федерации.

Статья предусматривает различные меры уголовной ответственности в зависимости от способов и субъектов преступления, а в случаях если такие действия повлекли тяжкие последствия, то виновному грозит наказание до 10 лет лишения свободы.

**Люберецкая городская прокуратура разъясняет**

# **О мерах защиты от преступлений, совершаемых с использованием информационно-коммуникационных технологий**

В нынешний период банковская система все больше уделяет внимание упрощающим жизнь человека высоким технологиям, активно внедряя их в различные операционные процессы для взаимодействия финансового учреждения с многочисленными клиентами. Наиболее популярны телефонные приложения, с помощью которых можно в любое время суток осуществлять банковские операции, оплатив, например, через личный кабинет с помощью банковской карты любой товар в интернет-магазинах.

Вместе с тем усиливающаяся информатизация современного общества имеет и негативные последствия, заключающиеся в появлении и росте особых разновидностей правонарушений, злоумышленники, в свою очередь, не стоят на месте.

Одна из таких групп преступных посягательств выражается в совершении различных корыстных действий (бездействия) в сферах информационных технологий с применением компьютерной информации, электронных (цифровых) технологий и т.п.

Чтобы не стать жертвой преступников применяйте эти простые правила:

— не сообщайте свои персональные данные, а также банковских карт и счетов третьим лицам, даже если неустановленное лицо представилось сотрудником банка, прекратите разговор и обратитесь в банк лично либо по телефону горячей линии;

— не выполняйте указания неизвестных лиц по вводу каких-либо команд и символов в телефонном режиме, а также с использованием банкомата;

— не перечисляйте денежные средства неизвестным лицам, представляющимся знакомыми ваших родных, сотрудниками правоохранительных органов (положите трубку и позвоните лицу, который по словам неизвестного попал в беду/нуждается в помощи);

— прежде чем приобретать какой-либо товар или услугу с использованием сети «Интернет», ознакомьтесь с отзывами, оставленными ранее покупателями/клиентами;

— при вводе пин-кода банковской карты закрывайте его рукой, не храните пин-код совместно с банковской картой.