Российская Федерация
Свердловская область
Управление образования
Администрации
муниципального образования
«Каменский городской округ»
623409, Свердловская область,
г. Каменск-Уральский,
ул. Революционная, 13
E-mail: uo_priomnaja@mail.ru
тел. (3439) 36-50-73
от 24.12.2020 № 1087
на № _____ от _____

Специалистам Управления образования, МКУ «ЦСО», МКУ «Централизованная бухгалтерия»

Руководителям образовательных организаций

О направлении информации

Уважаемые коллеги!

В связи с ростом хищений, совершаемых с использованием информационно-коммуникационных технологий, во исполнение письма прокуратуры Управление образования Администрации муниципального образования «Каменский городской округ» (далее - Управление образования) сообщает Вам следующую информацию.

Развитие технологий в современном мире обуславливает их проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, в том числе личное обогащение.

Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, у физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа хищения предусмотрена ст.ст. 158, 159, 159.3, 159.6 Уголовного кодекса РФ.

Мошенники используют разные способы обмана людей в интернете: от спама до создания сайтов-двойников. Цель злоумышленников — получить персональные данные пользователя, номера банковских карт, паспортные данные, логины и пароли.

Законодателем в целях сдерживания роста указанного рода хищений внесены изменения в российское уголовное законодательство. Так, Федеральным законом от 23.04.2018 г. внесены изменения в часть 3 статьи 158 Уголовного кодекса РФ, устанавливающей уголовную ответственность за тайное хищение чужого имущества, статья дополнена квалифицирующим признаком: «деяние, совершенное с банковского счета, а равно в отношении электронных денежных средств». Одновременно в новой редакции изложена статья 159.3 Уголовного кодекса РФ, предусматривающая уголовную ответственность за мошенничество с использованием электронных средств платежа.

Подчеркивая общественную опасность преступлений, связанных с мошенничеством с использованием электронных средств платежа и в сфере компьютерной информации, законодателем снижен нижний порог значения совершения преступления с причинением крупного размера с одного миллиона пятисот тысяч рублей до двухсот пятидесяти тысяч рублей, особо крупного размера – до одного миллиона рублей.

Рассматриваемые хищения денежных средств с банковских счетов граждан, совершенных с использованием систем дистанционного банковского обслуживания, можно разделить на группы:

- субъект осуществляет телефонный звонок от лица вымышленных сотрудников банка или службы безопасности и сообщает о необходимости предоставления информации о номере карты, ее владельце, сроке действия, трехзначном коде, указанном на оборотной стороне карты, в связи с «проведением профилактических работ», «блокированием карты по подозрению в попытке хищения денег» и т.п.;
- субъект просит предоплату за товар или услуги в Интернете;
- субъект сообщает о выигрыше;
- субъект осуществляет телефонный звонок лицу и сообщает, что у его родственника (знакомого) проблемы, например, попал в ДТП, совершил правонарушение и т.п., и предлагает «решить проблему» с помощью внесения на счет злоумышленника определенной денежной суммы.

Следует отметить, что число указанных противоправных деяний продолжает увеличиваться. Высокая степень общественной опасности таких преступлений подтверждается их спецификой - совершить их могут лица, обладающие специальными знаниями и использующие технические средства именно в криминальных целях, что приводит к нарушению не только права собственности, но и банковской тайны.

Необходимо быть крайне бдительными. Сотрудник банка не имеет право спрашивать пароль от карты и уж тем более, его нельзя никому сообщать. Чтобы не стать жертвой подобной аферы, достаточно повесить трубку и перезвонить в банковскую организацию по телефону, указанному на официальном сайте или на обороте карты. Уточните у оператора, действительно ли кто-то пытается снять деньги и сообщите номер телефона мошенников.

Будьте внимательны! Пользуйтесь последними версиями браузеров и лицензионного антивирусного программного обеспечения. Следите за тем, чтобы при входе на сайты было установлено защищенное соединение https.

О подобных фактах следует незамедлительно сообщать в правоохранительные органы, в первую очередь – в полицию. Такие сообщения тщательно проверяются в целях установления лиц, причастных к преступной схеме, и их привлечения к уголовной ответственности.

Управление образования в дополнение к вышеизложенному направляет памятки для ознакомления.

Приложение: на 4х л. в 1 экз.

Начальник Управления образования С.В. Котышева

Оксана Викторовна Павловских
юрисконсульт МКУ «Центр сопровождения образования»
(3439) 36-40-45

Предупреждение компьютерных преступлений

3

Известно много мер, направленных на предупреждение преступления. Выделим из них:

- Технические

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев.

- Организационные

К организационным мерам отнесем охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком.

- Правовые.

К правовым мерам следует отнести: разработку норм, устанавливающих ответственность за компьютерные преступления; защиту авторских прав программистов; совершенствование уголовного и гражданского законодательства, а также судопроизводство.

Ответственность за правонарушения в сети интернет

РАСПРОСТРАНЕНИЕ ЭКСТРЕМИСТСКИХ МАТЕРИАЛОВ

Статья 20.29. Производство и распространение экстремистских материалов
Административный штраф в размере от 1000 –3000 т.р.
Административный арест на срок до 15суток с конфискацией указанных материалов и оборудования, использованного для их производства

НЕЗАКОННАЯ РЕКЛАМА НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

Статья 6.13 Пропаганда наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ
Административный штраф в размере от 4 –5 т.р. с конфискацией рекламной продукции и оборудования, использованного для ее изготовления.

НАРУШЕНИЕ АВТОРСКИХ ПРАВ

Статья 146. Нарушение авторских и смежных прав
Штраф до 200 т.р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательные работы на срок до 480 часов, либо исправительные работы на срок до 1 года, либо арест на срок до 6 месяцев.

КЛЕВЕТА В СЕТИ ИНТЕРНЕТ

Статья 152. Защита чести, достоинства и деловой репутации
Штрафные санкции до 1 млн. р. или размер заработка в общей сумме до 1 года. Обязательные работы в совокупности до 240 часов.

РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И СВЕДЕНИЙ О ЧАСТНОЙ ЖИЗНИ

Статья 137. Нарушение неприкосновенности частной жизни
Штраф в размере до 200 000 руб., обязательные или исправительные работы на срок до 360 часов или до 1 года; арест до 4 месяцев; лишение свободы до 2 лет.

МОШЕННИЧЕСТВО, СВЯЗАННОЕ С БЛОКИРОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРОВ ПОЛЬЗОВАТЕЛЕЙ

Статья 272. Неправомерный доступ к компьютерной информации
Штраф до 200 т.р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательные работы на срок до 480 часов, либо исправительные работы на срок от 6 мес. до 1 года, либо лишение свободы на срок до 2 лет.
Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ
Лишение свободы до 3 лет со штрафом от 200 т.р. или в размере заработной платы или иного дохода осужденного за период до 18 месяцев.

ХИЩЕНИЯ, СОВЕРШАЕМЫЕ С ПОМОЩЬЮ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Статья 272. Неправомерный доступ к компьютерной информации
Штраф до 200 т.р. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительные работы на срок до 1 года, либо ограничение свободы на срок до 2 лет, либо принудительные работы на срок до 2 лет, либо лишение свободы на тот же срок.

Компьютерные преступления - это преступления, совершенные с использованием компьютерной информации. При этом, компьютерная информация является предметом и (или) средством совершения преступления

Классификация компьютерных преступлений:

@ Неправомерный доступ к охраняемой законом компьютерной информации.

@ Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

@ Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Преступления в сфере информационных технологий включают:

- распространение вредоносных вирусов
- взлом паролей;
- кражу номеров банковских карт и других банковских реквизитов (фишинг);
- распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет;
- вредоносное вмешательство через компьютерные сети в работу различных систем;
- интернет-аукционы, в которых сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара.