«Киберпреступность:
понятие, виды, как распознать, способы защиты»

Киберпреступление – это противоречащая закону деятельность, которая направлена на атаку компьютерной техники, компьютерной сети или сетевых устройств.

Целью киберпреступности (как правило) является получение финансовой прибыли. Также целью может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов.

Для примера можно привести некоторые разновидности киберпреступлений:

- мошенничество с использованием электронной почты и интернета;
- кража цифровой личности (хищение и использование личных данных);
- кража данных платежных карт и другой финансовой информации;
- хищение и перепродажа корпоративных данных;
- кибершантаж (вымогательство денег под угрозой атаки, атаки с использованием программ-вымогателей);
- криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);
- кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);
- нарушение работы систем с целью компрометации сети;
- нарушение авторских прав и т.д.

Киберпреступления всегда характеризуются повышенной скрытность совершения преступления, которая обеспечивается спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.).

Киберпреступления имеют трансграничный характер сетевых преступлений, при котором преступник, объект преступного посягательства, потерпевший могут находиться на территориях разных государств.

Для киберпреступлений также характерны:

- особая подготовленность преступников, интеллектуальный характер преступной деятельности,
- нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств,
- возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно.
- многоэпизодный характер преступных действий при множественности потерпевших.
- неосведомленность потерпевших о том, что они подверглись преступному воздействию.
- дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

Способы защиты от киберпреступлений:

- регулярное обновление ПО и операционной системы;
- использование антивирусных программ и их регулярное обновление;
- использование надежных паролей;
- не открывать вложенные файлы в письмах;
- не переходить по ссылкам в спам-письмах и на незнакомых веб-сайтах;
- осторожность при передаче личной информации;
- общение по официальным каналам;
- внимательность при посещении веб-сайтов;
- регулярная проверка банковских выписок.

В настоящее время особо актуальной становится проблема **защиты аккаунтов** в социальных сетях и противодействия различным формам и видам мошенничества. Наиболее типичные способы обмана в соцсетях сегодня таковы:

Предоплата - злоумышленники размещают объявления о продаже каких-либо товаров по низким ценам, но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

Шантаж и вымогательство **-** некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства. Социальные сети – это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в интернете.

Онлайн-игры - индустрия производства игр для персональных компьютеров и мобильных гаджетов давно стало высокодоходным бизнесом. Не удивительно, что повышенным вниманием она пользуется и у мошенников. Ценность тут представляют и аккаунты пользователей, к которым нередко привязаны реквизиты БПК для покупки игровых преимуществ, и коллекционные предметы, которые игроки также нередко приобретают за реальные деньги.

Также людям звонят якобы от *имени работников городских поликлиник,* чтобы сообщить о серьезных проблемах по результатам анализов. И жертвы, опасаясь за свое здоровье, соглашаются на покупку дорогостоящих лекарств. Однако после оплаты и получения своей покупки потерпевшие спустя некоторое время обнаруживали, что приобрели безвредные пищевые добавки.

Новым способом мошенничества с кражей личных данных стало создание мошенниками *фейковых сайтов якобы для выплаты детских пособий,* после регистрации на которых граждане выдают им все персональные данные из кабинета на сервисе "Госуслуги". Киберпреступники

воспользовались ситуацией: они создают новые сайты, якобы приспособленные для выплаты пособий, рассылают СМС и электронные письма с призывом пользоваться их сервисом для оформления выплат. Вводя свой логин и пароль на сайте-дублере, граждане предоставляют мошенникам доступ ко всем своим данным, хранящимся в личном кабинете на официальном портале "Госуслуги".

При этом, фейковые сайты могут отличаться доменным именем, одной буквой или цифрой в адресе от официального портала.

Прокуратура города настоятельно рекомендует гражданам внимательно проверять адресную строку браузера при заходе на Интернет-ресурс и установить на компьютер антивирусную программу. Бдительно относится к предоставлению своих персональных данных.

В случае возникших у Вас подозрений о законности совершаемых в отношении Вас действий незамедлительно сообщать в правоохранительные органы.

Прокуратура города Котовска.