Рекомендации для пользователей сети Интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

- для выхода в сеть Интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;

- используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения;

- при использовании известных Вам сайтов, обращайте внимание на их внешний вид: возможно, Вы зашли на поддельную его копию;

- вводите личную информацию только на веб-сайтах, работающих с использованием защищенных протоколов (обычно в браузере рядом с адресом такого сайта отображается значок замка на зеленом фоне);

- не используйте одинаковые логины и пароли на различных сайтах;

- не используйте слишком легкие пароли, либо те, о которых можно легко догадаться (даты рождения, номера телефонов и т.д.);

- по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

- остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель, никогда не открывайте вложения и не переходите по ссылкам в таких сообщениях;

- с осторожностью относитесь к письмам, в которых запрашиваются данные счетов (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), никогда не отправляйте финансовую информацию по незащищенным Интернет-каналам;

- при поступлении сообщений от знакомых, содержащих побуждение к осуществлению финансовых транзакций либо передаче финансовых реквизитов, обязательно необходимо проверить данную информацию с использованием других каналов связи (личная встреча, телефонный звонок, мессенджер, поддерживающий голосовую связь), либо, в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;

- если Вы не используете банковскую платежную карточку для осуществления Интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

- при осуществлении Интернет-платежей по возможности используйте технологии обеспечения дополнительной безопасности платежей, такие как 3-D Secure для международных платежных систем Visa и MasterCard или Интернет Пароль для платежной системы БЕЛКАРТ.

В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная, за совершение противоправных деяний в сфере высоких технологий.

Уголовным кодексом предусмотрен ряд преступлений, отнесенных к компетенции подразделений по раскрытию преступлений в сфере высоких технологий. Рассмотрим их подробнее.

Статья 212. Хищение путем использования компьютерной техники

Необходимо отметить, что ответственность за деяния, предусмотренные ст.212, наступает с 14-летнего возраста.

Примером такого преступления может быть хищение денежных средств с найденной либо похищенной банковской платежной карточки с использованием банкомата, платежного терминала. В последнее время все чаще фиксируются факты хищений с использованием реквизитов карт при осуществлении Интернет-платежей, а также завладение денежными средствами, хранящимися на счетах различных электронных платежных систем и сервисов.

Статья 349. Несанкционированный доступ к компьютерной информации

Например – несанкционированный доступ (открытие и просмотр файлов, писем, переписки) к электронной почте, учетным записям на различных сайтах,

в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350. Модификация компьютерной информации

В качестве примера можно привести произведенные изменения компьютерной информации: переписка в электронной почте, в социальной сети, в мессенджере с правами другого пользователя; изменение текстовой, графической и иной информации; внесение изменений в защищенные базы данных и т.д.

Статья 351. Компьютерный саботаж

Здесь мы говорим об умышленном уничтожении (удалении, приведении в непригодное состояние, шифровании) компьютерной информации либо ее блокировании (например путем смены пароля доступа, изменении графического ключа и т.д.).

Статья 352. Неправомерное завладение компьютерной информацией

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации, повлекшие причинение существенного вреда. К примеру – копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами фотографий с компьютера.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов, например поддельных смарт-карт для просмотра закодированных каналов спутникового телевидения.

Статья 354. Разработка, использование либо распространение вредоносных программ

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

Указанная статья применяется к лицам, имеющим доступ к компьютерным сетям и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем.

Ответственность за деяния, предусмотренные ст.ст.349-355 наступает с 16-летнего возраста.

Алгоритм действий, которые помогут не стать жертвой мошенников:

- не соглашаться на предложение случайных знакомых погадать, снять порчу, избавить от наложенного на близких заклятия;
- не пускать в квартиру не знакомых лиц, в том числе представляющихся работниками социальных, газовых, электроснабжающих служб, за исключением случаев, если сами вызывал и их. Перезвоните и уточните, направляли ли к Вам этого специалиста;
- не верить телефонным звонкам с неизвестных номеров о том, что Ваш родственник, близкий или знакомый совершили или пострадали в ДТП, стали соучастниками преступления, и за решения вопроса о привлечении их к ответственности необходимы деньги. Задайте звонящему вопросы личного характера, помогающие отличить близкого человека от мошенника. Под любым предлогом прервать контакт с собеседником и перезвонить родным и узнать, все ли у них в порядке.
- не разглашать свои персональные данные, такие как фамилия, имя, отчество, паспортные данные, данные банковских карт, счетов, а также защитные коды и пароли, ни под каким предлогом;
- не передавать деньги не знакомым лицам, не под каким предлогом;

- не соглашаться на предложение обменять деньги на новые или иностранные купюры; рассказы о грядущей денежной реформы не правда;

- не доверять СМС-сообщениям, приходящим на телефон, будь то крупный выигрыш, победа в конкурсе или лотереи, особенно в тех случаях, когда для получения выигрыша просят оплатить налог; необходимо знать, что настоящий розыгрыш призов не должен подразумевать денежные выплаты с Вашей стороны;

- не перезванивать на номер, с которого пришло СМС-сообщение о том, что банковская карта заблокирована и не отправлять ответных смс-сообщений; решение в данной ситуации позвонить в банк, выпустивший и обслуживающий карту (телефон банка указан на обороте банковской карты);

- не отправлять денежные средства на неизвестные адреса, в том числе с целью приобретения вещей в сети Интернет;

- избегать лиц, которые навязчиво пытаются вовлечь в разговор, предлагают какие-либо товары и услуги или же хотят поделиться с найденными деньгами;

- избегать внимание людей при снятии денег с карты или книжки.