

Профилактика и предупреждение преступлений в сфере информационно-телекоммуникационных технологий

Информационно-телекоммуникационные технологии (ИТТ) играют огромную роль в современном обществе и оказывают значительное влияние на различные аспекты жизни людей.

Во-первых, ИТТ позволяют существенно улучшить доступ к информации. С появлением Интернета и широкого распространения цифровых технологий стало возможным получать информацию из разных источников по всему миру всего лишь за несколько кликов. Это создает безграничные возможности для образования, самообразования, профессионального развития и культурного обогащения.

Во-вторых, ИТТ играют важную роль в коммуникации и обмене информацией. Они упрощают и ускоряют передачу сообщений, позволяют общаться с людьми по всему миру через электронную почту, социальные сети, видео- и аудиозвонки.

Тем не менее, следует отметить, что интенсивная цифровизация общества и связанное с ним расширение сфер применения ИТТ создают «благоприятную» среду для возникновения новых способов совершения преступлений, таких как:

1. Кибермошенничество: различные схемы обмана и мошенничества: фишинговые сообщения, ложные звонки «служб поддержки» и т.д.
2. Киберпроникновение (хакинг): проникновение в компьютерные системы или сети для получения незаконного доступа к данным, вреда или кражи информации для вымогательства денег, блокировки доступа к компьютеру или файлам, шифрование данных или угрозы публикации скомпрометированной информации.
3. Кибербуллинг: использование ИТТ для травли, угроз или домогательств в сети Интернет: публикация негативных сообщений, клеветы, манипуляция фотографиями и другие формы психологического насилия.
4. Кибертерроризм: использование ИТТ для создания паники, страха и нарушения общественной безопасности.

Виртуальное пространство предоставляет пользователям возможность взаимодействовать и общаться в онлайн-среде без раскрытия своей реальной личности, что приводит к возникновению ложного чувства анонимности и способствует проявлению негативных поведенческих тенденций.

При совершении преступлений преступники используют различные поводы, чтобы завладеть информацией или побудить человека самостоятельно передать денежные средства. Типичными фразами, предложениями для осуществления преступлений являются: «Ваш родственник попал в беду», «Ваша организация будет подвергнута проверке определенными органами», классическое, но действенное «с Вашего банковского счета происходят операции по списанию», «Вам ошибочно переведены деньги», «Вы участвуете в акции и выиграли приз», «Положи мне на телефон деньги, не могу до тебя дозвониться», «Ваш почтовый ящик заблокирован, срочно перейдите по ссылке»,

«Ваши инвестиции и Ваш бизнес – гарантия отличного дохода», «Вы можете предупредить преступление» и т.д.

Участились случаи звонков якобы из службы безопасности банка о совершении подозрительных операций, когда преступники получают персональные данные потерпевшего, доступ к его счетам, с которых списывают денежные средства или оплачивают в интернет-магазинах.

Часто преступники звонят гражданам, обращаются к ним по фамилии, имени, отчеству, сообщают, что в отношении них либо их близких родственников возбуждено уголовное дело или проводится проверка, в связи с чем возникла необходимость получить данные для аутентификации в системах дистанционного банковского обслуживания, сведения о совершенных по карте операциях или любые другие сведения.

Сравнительно новым случаем является звонок потерпевшему из «службы безопасности банка», а после – звонок от сотрудников правоохранительных органов и сообщение о совершении в отношении потерпевшего преступления со стороны сотрудников банка под предлогом предотвращения несанкционированных действий. Мошенники убеждают потерпевшего оформить кредит, обналичить денежные средства и перевести на якобы защищенный специально созданный расчетный счет.

Распространены случаи хищений денежных средств путем оформления онлайн-кредитов при установке гражданами программ удаленного доступа к своим электронным устройствам и передаче прав управления ими третьим лицам. Мошенники, используя психологические и социальные приёмы и методы «атаки на человека», убеждают граждан установить компьютерные программы TeamViewer и QuickSupport либо их аналоги на свои электронные устройства, после чего получают контроль над этими устройствами и совершают хищения, оформляя онлайн-кредиты.

В преступных целях также используются различные интернет-сервисы для размещения объявлений (Avito, Юла, Drom, BlaBlaCar и другие). Преступные действия осуществляются под предлогом перевода средств в счет оплаты товара либо осуществления предоплаты за товар, а также каких-либо услуг по фиктивной доставке товара.

В подобных ситуациях злоумышленники получают персональные данные гражданина, иную конфиденциальную информацию, после чего получают доступ к их личным кабинетам в мобильных банковских приложениях, осуществляют переводы, совершают покупки с его счета в банке.

Также имеются случаи, когда потерпевшие самостоятельно перечисляют на счета преступников свои деньги для прекращения уголовного преследования или процессуальной проверки.

В современных реалиях необходимо развивать навыки цифровой гигиены, соблюдение базовых принципов которой позволит минимизировать уровень негативного влияния медиапространства, что является важным аспектом благополучия.

Одной из основных составляющих цифровой гигиены является поддержание электронной безопасности.

Это включает в себя использование надежных паролей и их регулярное обновление, а также активацию двухфакторной аутентификации для защиты личных данных от несанкционированного доступа.

Также следует воздержаться от общения с неизвестными пользователями, от распространения информации личного характера о себе и своих близких, не ставить отметки о геолокации, относиться с подозрением к электронным сообщениям, требующим немедленно перейти по ссылке, позвонить или открыть вложение, перевести деньги или оплатить выигрыш.

Ни при каких обстоятельствах не следует передавать свои технические устройства незнакомым и малознакомым лицам, а при использовании Интернет-ресурсов не переходить по ссылкам на сомнительные сайты.

Не сообщайте посторонним лицам свои персональные данные, а также информацию о банковских картах и счетах (номера, коды доступа, пароли и т.д.), не берите по инициативе третьих лиц кредиты на своё имя и не переводите свои денежные средства либо кредитные на счета звонящих вам мошенников, представляющих сотрудников правоохранительных органов (прокуратуры, полиции и т.д.), социальных и иных служб, кредитных организаций.

Необходимо всегда помнить, что работники банков и правоохранительных органов не выясняют по телефону вопросы о денежных средствах на счетах граждан либо об их банковских картах. Сотрудники банков не звонят клиентам при сомнительных операциях, а сразу производят блокирование счета (карты).

Знайте, что преступники используют специальные программы подмены номера, в результате которой Вашим техническим устройством поступающие от преступников звонки определяются как принадлежащие банку и идентичные указанному на обороте банковской карты;

Когда вам звонят и под любым предлогом заводят разговор о финансах, знайте, что это мошенники. При поступлении таких звонков немедленно прерывайте соединение и не ведите разговор со звонящим.

В случае, если Вы стали жертвой мошеннических действий в сети Интернет – Вы вправе обратиться в суд с исковым заявлением о взыскании неосновательного обогащения с лиц, на счетах которых переведены Ваши денежные средства, если эти счета установлены правоохранительными органами; а также – с исковым заявлением о признании кредитного договора недействительным, в случае заключения Вами такого договора в результате мошеннических действий. В целях разъяснения порядка обращения с указанными заявлениями и получения иной правовой помощи Вы вправе обратиться в прокуратуру Алтайского района.

Будьте бдительны при общении по телефону и в сети Интернет.

Следует помнить, что Интернет — это публичное пространство, и вести себя в нем нужно точно также, как в любом другом общественном месте.