

Преступления в сфере информационных технологий включают в себя не только распространение вредоносных вирусов, взлом паролей, сайтов, кражу номеров кредитных карточек, но и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Краевое государственное бюджетное учреждение социального обслуживания «Комплексный центр социального обслуживания населения «Партизанский»

Наш адрес: с. Партизанское, ул. Гагарина, д. 30

Телефон: 8(39140) 22-1-36

Электронная почта:
mbucso47@mail.ru

Сайт:
<https://партизанский-центр.рф>



Краевое государственное бюджетное учреждение социального обслуживания «Комплексный центр социального обслуживания населения «Партизанский»

Мошенничество в сфере информационных технологий



Социально-реабилитационное
отделение

2022год

Схемы телефонного мошенничества:

- ♦ **Обман по телефону:** требование выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.



- ♦ **SMS-просьба о помощи:** требование перевести

определённую сумму на указанный номер, используется обращение «мама», «сынок», «друг» и т.д.

- ♦ **Выигрыш в лотерее,** который якобы проводит оператор связи: для получения приза Вас просят перевести определенную сумму на указанный номер телефона или счета и сообщить специальный код
- ♦ **СМС «Ваша карта временно заблокирована, перезвоните по номеру»:** Вам ответит мошенник и попытается узнать реквизиты банковской карты.

Если Вы сомневаетесь, что звонивший—действительно Ваш друг или родственник, постарайтесь перезвонить на его мобильный

Мошенничество в сети интернет

- ♦ **Онлайн покупки:** мошенники просят предоплату за несуществующий товар или услугу;
- ♦ **Дублирование сайтов (фишинг):** мошенники создают свой сайт (группу в соцсети) или копию сайта по продаже авиабилетов. При этом в реквизитах оплаты указывают свои банковские счета;
- ♦ **Лже-благотворительность:** интернет пестрит объявлениями о людях, нуждающихся в помощи, однако, не спешите перечислять деньги, не проверив необходимую информацию;
- ♦ **Работа в ИНТЕРНЕТЕ:** работодатели, которые предлагают Вам легкую работу за огромные деньги, не только не заплатят Вам ни копейки, но и обманным путем завладеют вашими деньгами;
- ♦ **Спам (нежелательное сообщение):** открывая такое сообщение, Вы выпускаете в свою систему компьютерный вирус-троян, который собирает информацию, а затем высылает ее спамерам, которые могут использовать полученное в своих целях.

Устанавливайте на свои ПК и мобильные устройства только лицензионное ПО

Мошенники в социальных сетях

- ♦ **Взлом аккаунта друга:** люди могут даже не подозревать, что им пишет посторонний человек. Таким образом, войдя в доверие, мошенники попытаются украсть Ваши деньги;
- ♦ **Схемы проведения аукционов в системе on-lain:** мошенники в соцсетях предлагают выслать деньги в оплату товара, а затем доставляют изделие намного менее ценное, чем то, которое было заявлено;
- ♦ **Группы «Отдам даром»:** Опасность может таиться в том, что мошенники попросят оплатить пересылку или «защиту от обмана». В результате Вы можете лишиться денежных средств.



Не распространяйте в соцсетях слишком подробную информацию о себе, это может отлично сыграть на руку мошенникам