



Прокуратура
Российской Федерации

ПРОКУРАТУРА
ОРЛОВСКОЙ ОБЛАСТИ
ПРОКУРАТУРА
ДМИТРОВСКОГО РАЙОНА

ул. Рабоче-Крестьянская, 8а, г. Дмитровск
Орловская область, 303240
телефон: 8 (48649) 2-14-57



327388 518316

Главе администрации Дмитровского
района,
главам администраций Алешинского,
Березовского, Бородинского, Горбуновского,
Домаховского, Друженского,
Столбищенского, Лубянского,
Малобобровского, Соломинского,
Плосковского, Долбенкинского сельских
поселений

03.02.2023 № 37-2023

На № _____ от _____

Уважаемые главы администраций!

Направляю для размещения на официальных сайтах администраций органов местного самоуправления разъяснение прокуратуры Дмитровского района «О профилактике правонарушений, совершаемых с использованием информационно-телекоммуникационных технологий»

Приложение на 1 л.

Заместитель прокурора района

советник юстиции

П.В. Постников

ОР № 007350

Прокуратура Дмитровского района Орловской
области
№ 37-2023/21-23-1321

Прокуратура Дмитровского района разъясняет о профилактике правонарушений, совершаемых с использованием информационно-телекоммуникационных технологий

В настоящее время всё актуальнее становятся вопросы связанные с хищением, совершенном с использованием современных информационно-коммуникационных технологий. Данный вид хищения является общественно опасным деянием, причиняющий имущественный вред гражданам и разрушающий нравственные устои общества.

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. У потерпевших похищаются денежные средства под предлогом совершения каких-либо банковских операций, направленных на восстановление якобы поврежденных данных об их банковских вкладах, либо путем введения их в заблуждение. При этом зачастую злоумышленники представляются банковскими работниками.

Анализ способов совершения преступлений с использованием информационно-телекоммуникационных технологий показал использования 3 схемы:

- схема - злоумышленник звонит или отправляет СМС-сообщение на телефоны, сообщая, что банковская карта или счет мобильного телефона потерпевшего заблокированы в результате преступного посягательства, и затем представляясь сотрудником банка или телефонной компании, предлагает набрать комбинацию цифр на мобильном телефоне или банкомате для разблокировки, в результате чего денежные средства перечисляются на счет преступника;

- схема - поступает звонок от «сотрудника» службы технической поддержки оператора мобильной связи с предложением подключить новую услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи абоненту предлагается набрать под диктовку код, который является комбинацией для перевода денежных средств со счета абонента на счет злоумышленника;

- схема - потерпевший заказывает товар через сеть Интернет, оплачивает его путем перечисления денежных средств на банковскую карту продавца, но не получает заказ.

С целью пресечения совершения преступления, необходимо критически относиться к таким сообщениям и не выполнять просьбы.

При возникновении подобной ситуации необходимо самостоятельно связаться с оператором банка, сотовой связи и узнать о совершении блокировки карты, номера телефона, отключении услуг и передать при наличии номер телефона злоумышленника. Данные действия поспособствуют незамедлительному установлению злоумышленника и пресечению совершения преступления.

Помните, что ни одна организация, включая банк, не вправе требовать реквизиты Вашей карты включая CVV-код!