ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА
АСТРАХАНСКОЙ ОБЛАСТИ
**ПРОКУРАТУРА
ГОРОДА АСТРАХАНИ**

ул. Советская, 5 Кирова, 21, г. Астрахань, 414000

684272 696209

Главе муниципального образования
«Город Астрахань»

Пермяковой М.Н.

19.02.2021 №127-2021/39-21-20120002

На № _____ от _____

Уважаемая Мария Николаевна!

Направляю в Ваш адрес буклет на тему: «Обезопась себя от Интернет-мошенников» для решения вопроса о размещении его на доске объявлений в целях предупреждения преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий.

О результатах рассмотрения информации прошу сообщить в прокуратуру г. Астрахани.

Приложение: на 1 л.

Заместитель прокурора города

советник юстиции Е.А. Авдеева

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 01D6756AD4338E200000034D119A0001
Владелец Авдеева Елена Анатольевна
Действителен с 18.08.2020 по 18.08.2021

Администрация муниципального образования
«Город Астрахань»
Управление контроля и документооборота
Отдел документооборота
Вх. № 3201-4629
«20» 02 2021 г.

Л.А. Зевакина

4826807141109

Прокуратура
Города Астрахани

414000
г. Астрахань, Кировский район,
ул. Кирова, 21

телефон
«прямой линии»:
(8512) 30-65-58

Эл.почта:
gorodprok@yandex.ru

Прокуратура города Астрахани предупреждает

Обезопась себя от Интернет-мошенников

г. Астрахань,
2021 год

Правила безопасности в интернете

Надо помнить, что помимо мошенничества существует множество других угроз, в частности, разнообразные вредоносные программы, которые могут и без «общения» мошенников с пользователем красть различные пароли, логины, информацию о кредитных картах и многое другое.

Для того чтобы обезопасить себя, любой пользователь Сети должен соблюдать несколько простых правил:

- **Пользоваться антивирусом:** современный, регулярно обновляемый антивирус обеспечит надежной защитой от разнообразных интернет-угроз;
- **Регулярно загружать обновления:** обновления программ закрывают уязвимости, которыми могут воспользоваться злоумышленники;
- **Не оставлять своих персональных данных на открытых ресурсах:** данные, оставленные в интернете, собирают роботы злоумышленников, которые в дальнейшем могут использовать их в своих целях (например, присылать на ваш почтовый ящик больше спама);
- **Не загружать ничего со случайных сайтов:** высока вероятность того, что вместе с загруженной программой/книгой/фильмом вы получите и вредоносную программу;
- **Не проходить по ссылкам в спамовых письмах:** такие ссылки зачастую ведут на мошеннические, либо зараженные вредоносными программами сайты;
- **Не открывать приложения в письмах, если есть хоть какие-то сомнения в надежности адресанта:** Высока вероятность того, что в приложении содержится вредоносная программа (даже если это документ Word);
- **Не пытаться «отписаться» от спама (особенно в том случае, когда в спамерском письме есть соответствующая ссылка):** избавиться от спама это не поможет, скорее наоборот. Существуют два наиболее вероятных варианта развития событий: 1) спамеры регулярно запускают автоматическую проверку и чистку своих баз от несуществующих адресов; отвечая на письмо, вы подтверждаете, что ваш адрес (который, был, возможно, подобран автоматически) действительно существует, его действительно читают. Это побудит спамеров внести его в отдельные, «чистые» базы, вследствие чего вам будет приходить еще больше спама; 2) пройдя по ссылке, вы попадете на зараженный сайт и получите вредоносную программу на свой компьютер;
- **Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег:** откликнувшись, вы или потеряете свои деньги, или, что гораздо хуже, окажетесь замешаны в преступные махинации.

Мошенничество, увы, неискоренимо. И на просторах интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.