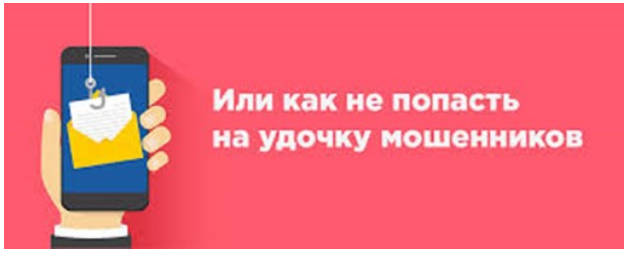
Меры предосторожности:

- не открывайте электронные письма от незнакомых отправителей или с подозрительными заголовками;
- используйте фильтры спама, предоставляемые почтовыми сервисами;
- не нажимайте на ссылки в спам-сообщениях и не отвечайте на них.

4. КИБЕРАТАКИ

Кибератаки – это нападения на компьютерные системы и сети с целью нанесения ущерба или получения несанкционированного доступа к конфиденциальной информации.

Кибератаки могут быть представлены в виде DDoS-атак, взлома паролей, кражи данных и других методов.



Меры предосторожности:

- используйте надежные пароли и регулярно их меняйте;
- включите брандмауэр на своем компьютере или сети (технологический барьер, который защищает сеть от несанкционированного или нежелательного доступа);
- регулярно обновляйте программное обеспечение и исправляйте уязвимости.

Будьте бдительны и примите необходимые меры для того, чтобы обезопасить свою информацию и компьютерные системы.

ОСТОРОЖНО!
Будьте бдительны, внимательны не поддавайтесь на уловки мошенников.
Если вы знаете о случаях мошенничества или сами стали жертвой злоумышленников, немедленно сообщите об этом в полицию по телефону 102.

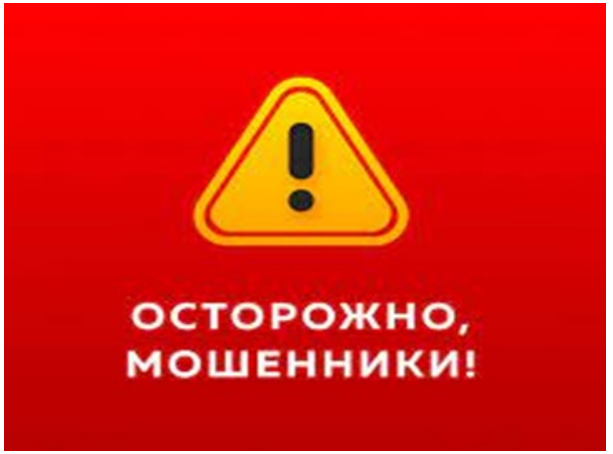
Если вы все-таки стали жертвой мошенников, немедленно сообщите об этом в полицию, позвонив по телефону 02, либо по телефону дежурной части 8(3452) 291-600.

УМВД России по Тюменской области
625000, г. Тюмень, ул. Водопроводная, 38,
тел. 8 (3452) 793-023 или 102,
тел. 8 (3452) 793-023 или 102
(для абонентов мобильной связи).

Совет при Тюменской областной Думе по повышению правовой культуры и юридической грамотности населения Тюменской области

УМВД России по Тюменской области

ПАМЯТКА



ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

г. Тюмень, 2024

Мошенничество в сфере информационных технологий представляет серьезную угрозу для пользователей и организаций. С развитием технологий и Интернета мошенники стали все более изобретательными и используют различные методы для обмана пользователей, таких как вредоносное программное обеспечение, фишинг, спам и кибератаки.

1. ВРЕДОНОСНОЕ ПО

Вредоносное программное обеспечение – это тип программного обеспечения, созданного с целью нанесения вреда пользователям или их компьютерам.

Оно может быть представлено в виде вирусов, червей, троянских программ и шпионского вредоносного программного обеспечения, оно может проникать на компьютер пользователя через вредоносные вложения электронной почты, загрузку с ненадежных веб-сайтов или уязвимость в программном обеспечении. Вредоносное программное обеспечение может причинить потерю данных, кражу личной информации и нарушение конфиденциальности.

Меры предосторожности:

- установка надежного антивирусного программного обеспечения и его регулярное обновление;
- осторожность при открытии вложений в электронной почте и загрузке файлов из Интернета;
- регулярное обновление операционной системы и программного обеспечения для исправления уязвимостей.

2. ФИШИНГ

Фишинг – это метод мошенничества, при котором злоумышленники выдают себя за доверенные организации или сервисы, чтобы получить доступ к личной информации пользователей, такой как пароли, номера кредитных карт и другие конфиденциальные данные.

Фишинг может осуществляться через фишинговые электронные письма, вредоносные веб-сайты или социальные сети.

Меры предосторожности:

- будьте осторожны при открытии электронных писем от незнакомых отправителей или с подозрительными ссылками;
- не предоставляйте личную информацию на ненадежных веб-сайтах или в ответ на подозрительные запросы;
- проверяйте URL-адреса веб-сайтов, чтобы убедиться, что они являются официальными.

3. СПАМ

Спам – это нежелательные и массовые электронные сообщения, которые могут содержать вирусы, фишинговые ссылки или другую вредоносную информацию.

Спам может приходить на электронную почту, в социальные сети или в виде всплывающих окон.