АНО «Центр поддержки и защиты детства»

ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Официальный сайт МВД по РМ

ОСНОВНЫЕ СОВЕТЫ ПО КИБЕРБЕЗОПАСНОСТИ

КИБЕРБЕЗОПАСНОСТЬ (ЕЕ ИНОГДА НАЗЫВАЮТ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТЬЮ) – ЭТО СОВОКУПНОСТЬ МЕТОДОВ И ПРАКТИК ЗАЩИТЫ ОТ АТАК ЗЛОУМЫШЛЕННИКОВ ДЛЯ КОМПЬЮТЕРОВ, СЕРВЕРОВ, МОБИЛЬНЫХ УСТРОЙСТВ, ЭЛЕКТРОННЫХ СИСТЕМ, СЕТЕЙ И ДАННЫХ.

КИБЕРБЕЗОПАСНОСТЬ НАХОДИТ ПРИМЕНЕНИЕ В САМЫХ РАЗНЫХ ОБЛАСТЯХ, ОТ БИЗНЕС-СФЕРЫ ДО МОБИЛЬНЫХ ТЕХНОЛОГИЙ.

В ЭТОМ НАПРАВЛЕНИИ МОЖНО ВЫДЕЛИТЬ НЕСКОЛЬКО ОСНОВНЫХ СОВЕТОВ.

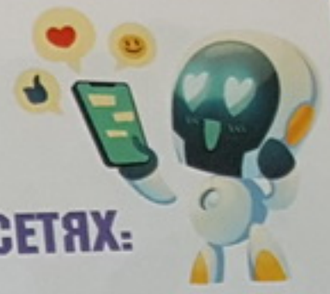
СОВЕТ 1. МЕТОДЫ ПО ЗАЩИТЕ ОТ ВРЕДОНОСНЫХ ПРОГРАММ:

1. Используй операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.
2. Работай на своем компьютере под правами пользователя, а не администратора.
3. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
4. Перед использованием внешних носителей информации (флешка, диск или файл из Интернета) обязательно проверяйте их на наличие вирусов.
5. Помни, компьютерные вирусы могут повредить или полностью уничтожить операционную систему со всеми файлами и данными в целом.

СОВЕТ 2.
БЕЗОПАСНОСТЬ ПРИ РАБОТЕ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI:

1. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту.
2. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам».
3. Используй только защищенное соединение через «https://», а не «http://».
4. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически».

СОВЕТ 3.
БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ:



1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
2. Не указывай в пароли телефоны, адреса, дату твоего рождения и другую личную информацию.
3. Защищай свою репутацию - подумай, прежде чем что-то опубликовать, написать и загрузить.
4. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.
5. Для социальной сети, почты и других сайтов используй разные пароли.

СОВЕТ 4. БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДЕНЬГАМИ:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету.
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.

СОВЕТ 5. БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ:

1. Надо выбрать правильный почтовый сервис и ставить сложный пароль.
2. Используй двухэтапную авторизацию (пароль и код из SMS).
3. Используй несколько почтовых ящиков (один- для частной переписки, другой – для регистрации на форумах и сайтах).
4. Не открывай подозрительные файлы и другие вложения в письмах. Если прислал твой знакомый, уточни у него, отправлял ли он их.
5. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

СОВЕТ 6. БЕЗОПАСНОСТЬ В МОБИЛЬНОМ ТЕЛЕФОНЕ:

1. Будь осторожен при предложениях бесплатного контента, в нем могут быть скрыты платные услуги.
2. Прежде чем отправить SMS, фото или видео, подумай, ты точно знаешь, где они будут в конечном итоге?
3. Используй антивирусные программы для мобильных телефонов.
4. Не загружай приложения от неизвестного источника.
5. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
6. Периодически проверяй какие платные услуги активированы на твоем номере.

СОВЕТ 7. БЕЗОПАСНОСТЬ В БОРЬБЕ С КИБЕРБУЛЛИНГОМ -

(виртуальное издевательство - преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство):

1. Не бросайся в бой. Лучший вначале успокоиться и посоветоваться как себя вести.
2. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
3. Веди себя вежливо. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
4. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
5. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

СОВЕТ 8. БЕЗОПАСНОСТЬ В БОРЬБЕ С ФИШИНГОМ:

1. Если тебя взломали, то необходимо предупредить об этом всех своих знакомых и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.

3. Установи надежный пароль (PIN) на мобильный телефон.

4. Отключи сохранение пароля в браузере.

СОВЕТ 9. БЕЗОПАСНОСТЬ ПРИ ПОКУПКАХ В ИНТЕРНЕТЕ:

1. Если не уверен в подлинности продавца- не производи предоплату товара и не вводи данные карты, особенно CVV-код на обороте.

2. Если на сайте прописаны только форма обратной связи и телефон продавца, такой магазин может предоставлять опасность.

3. Не следует поддаваться на слова «Акция», «Успей купить», «Предложение ограничено», стоимость товара в магазинах мошенников существенно занижена.

4. Отсутствие доставки и самовывоза на сайтах мошенников зачастую приводит к тому, что тебе придется оплатить услуги транспортной компании.

5. При продаже товара не сообщай мошенникам - покупателям данные банковской карты или смс-код!

ЕСЛИ ТЫ ИЛИ ТВОИ ЗНАКОМЫЕ СТАЛИ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ, НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В МВД ПО РЕСПУБЛИКЕ МОРДОВИЯ ПО ТЕЛЕФОНАМ:

02 - ПОЛИЦИЯ

112 - ЕДИНАЯ СЛУЖБА СПАСЕНИЯ

8 (8342) 29-80-88 - ТЕЛЕФОН ГОРЯЧЕЙ ЛИНИИ МВД ПО РМ

Брошюра подготовлена АНО «Центр поддержки и защиты детства» в рамках реализации проекта «Школа кибербезопасности»

Подписано в печать 14.02.2022 г. Формат 60x84/32.
Тираж 10000 шт. Заказ № 50

Отпечатано с оригинал-макета заказчика
в типографии ООО «Консоль»
430005, РМ, г. Саранск, ул. Б. Хмельницкого., д. 14, оф. пом. №2
тел.: 8 (8342) 24-60-61