ГУ «Комплекс «Музыкальный коледж – музыкальная школа – интернат для одарённых детей»

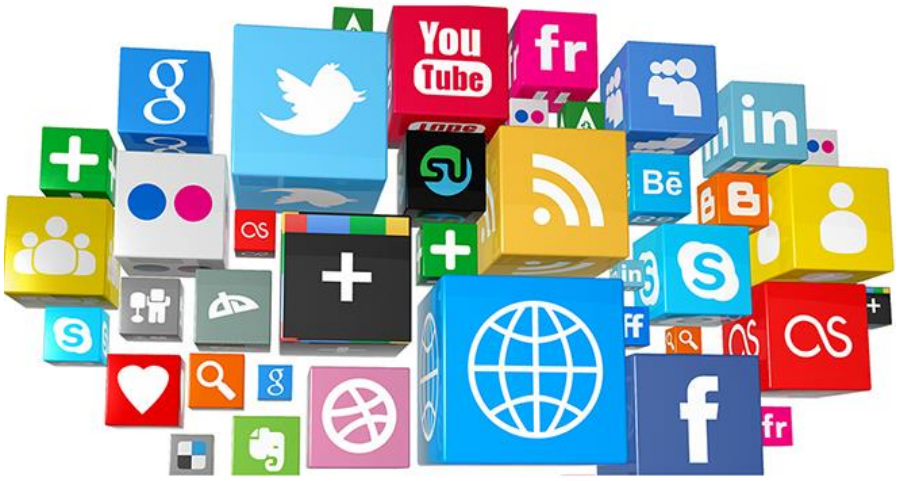
Методические рекомендации по кибербезопасности

Павлодар 2021

ПАМЯТКА 1.

Как безопасно общатся в социальных сетях

1. **Ограничить список друзей.** У тебя в друзьях не должно быть случайных и незнакомых друзей.
2. **Защищай свою частную жизнь.**Не указывай пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.
3. **Защищай свою репутацию.** Держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели то, что ты загружаешь? Подумай, прежде чем-то опубликовать, написать и загрузить.
4. **Не исопользуй реальное имя.** Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительство, место учебы и прочее.
5. **Не сообщай свое место положение.** Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.
6. **Используй сложные пароли.** При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строНе кчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.
7. **Используй разные пароли.** Для социальной сети, почты и других сайтов создавай новые пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всему сразу.



ПАМЯТКА 2.

Как безопасно пользоваться электронной почтой.

1. **Выбери правильный почтовый сервис.** В интернете много бесплатных. Однако почту лучше заводить на популярном сервисе, которым уже пользуются твои знакомые.
2. **Не пиши о себе в адресе почты.**Не указывай в почтовом адресе личную информацию. Например, лучше выбрать «музыкальный_фанат@»или «рок2018@» вместо «андрей2005@»
3. **Используй двухэтапную авторизацию.** Для двухэтапной авторизации помимо пароля нужно вводить код, который присылают по СМС.
4. **Выбери сложный пароль.** Для каждого почтового ящика должен быть свой сложный, устойчивый к взлому пароль.
5. **Используй проверочный вопрос.** Придумай сам свой личный вопроос для идентификации, если сервис дает такую возможность.
6. **Заведи несколько почтовых ящиков.** Первый для частной переписки с адресатами, которыми ты доверяешь. Этот электронный адрес не нужно использовать при регистрации на форумах и сайтах.
7. **Не открывай вложения писем.** Не открывай файлы и другие вложения в письмах, даже если они пришли от друзей. Уточни у них, отправляли ли они тебе эти файлы.
8. **Выходите из почты.** Не забывай нажимать «Выйти» после окончания работы на почтовом сервисе, перед тем как закрыть вкладку с сайтом.

ПАМЯТКА 3.
Как защититься от кибербуллинга

КИБЕРБУЛЛИНГ – ситуация, когда человека в Сети преследует сообщениями, которые содержат оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование.

1. **Не бросайся в бой.** Лучший способ: посоветоваться, как себя вести, и если нет того, к кому можно обратиться, то вначале нужно успокоится. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
2. **Управляй своей киберрепутацией.** Ищи способы выяснить, кто стоит за анонимным аккаунтом обидчика. Анонимность в Сети мнимая.
3. **Береги виртуальную честь с молоду.** Не веди хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет сложно.
4. **Игнорируй единичный негатив.** Однаразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
5. **Блокируй агрессора.** В программах обмена мгновенными сообщениями, в социальных сетях можно запретить конкретным адресам присылать сообщения.
6. **Поддержи жертву кибербуллинга.** Покажи преследователю, что оцениваешь его действия негативно. Сообщи взрослым о факте агрессивного поведения в Сети.

ПАМЯТКА 4.
Как защититься от компьютерных вирусов.

КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

1. **Загрузи современную операционную систему.** Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.
2. **Обновляй операционную систему.** Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.
3. **Используй права пользователя.** Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установится.
4. **Не рсикуй.** Используй антивирусные программные продукты проверенных производителей с автоматическими обновлением баз.
5. **Ограничить доступ к своему компьютеру.** Не разрешай посторонним пользоваться своим компьтером.
6. **Выбирай тщательно источники.** Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.

ПАМЯТКА 5.
Как безопасно пользоваться сетью Wi-Fi

Wi-Fi – это беспроводной способ передачи данныхъ с помощью радиосигналов. В кафе, отелях, аэропортах часто можно бесплатно выйти в интернет черезWi-Fi небезопасны. Но общедоступные сети Wi-Fi небезопасны.

1. **Не передавай личную информацию через общедоступные сети Wi-Fi.**Желательно не вводить пароли доступа, логины и номера.
2. **Используй и обновляй антивирусные программы и брандмауэр.** Так ты обезопасишь себя от закачки вируса на устройство.
3. **Отключи функцию «Общий доступ к файлам и принтерам» при использовании Wi-Fi.** Эта функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.
4. **Не используй публичный Wi-Fi для передачи личных данных.** Например, для выхода в социальные сети или в электронную почту.
5. **Используй только защищенное соединение через HTTPS, а не HTTP.** То есть при наборе веб-адреса вводи именно «https://».
6. **Отключи функцию «Подключение к Wi-Fi автоматически» в мобильном телефоне.** Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

ПАМЯТКА 6.
Как безопасно расплачиваться электронными деньгами.

ЭЛЕКТРОННЫЕ ДЕНЬГИ – это удобный способ платежей, однако за ними часто охотятся мошенники. В России закон разделяет электронные деньги на два вида – анонимные и персонифицированные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в персонифицированных идентификация пользователя обязательна.

1.Привяжи к счету мобильный телефон. Это самый удобный способ восстановить ему доступ. Привязанный телефон поможет, если забудешь платежный пароль или зайдешь на сайт с незнакомого устройства.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.

3. Придумай сложный пароль. Преступникам будет не просто угадать сложный пароль. Сложные пароли – это пароли, которые содержать не менее восьми знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак. Например, StROng!;;

4. Береги личные данные. Не вводи их на сайтах, которым не доверяешь.

ПАМЯТКА 7.

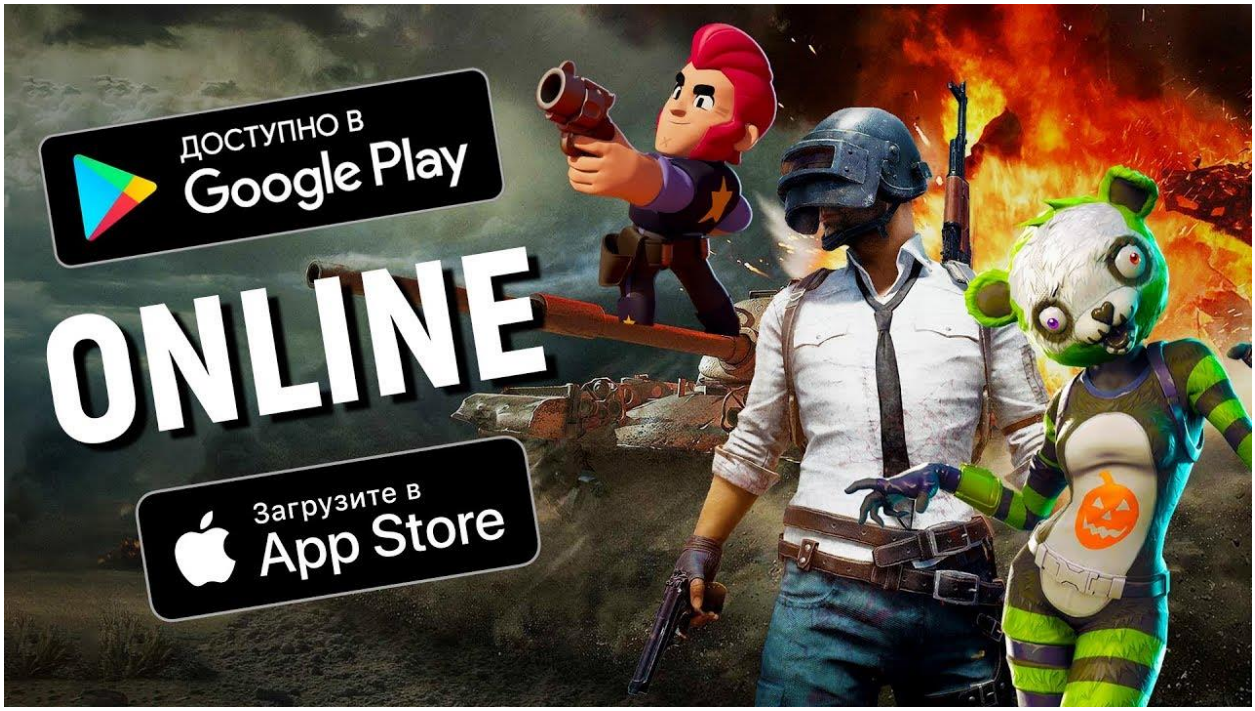
Как безопасно пользоваться смартфоном, планшетом.

1. **Будь осторожен.** Когда тебе предлагают бесплатный контент, в нем могут быть скрыты платные услуги.
2. **Думай, прежде чем отправить СМС, фото или видео.** Ты точно знаешь , где окажутся в конечном итоге?
3. **Обновляй операционную систему смартфона.** Это дополнительная защита.
4. **Используй антивирусные программы для смартфонов.** Регулярно обновляй их.
5. **Не загружай приложения от неизвестного источника.** Они могут содержать вредоносное программное обеспечение.
6. **Зайди в настройки браузера и удали cookies.** Сделай это сразу после того, как ты выйдешь с сайта, где вводил личную информацию.
7. **Проверяй платные услуги на твоем номере.** Иногда могут активировать новые.
8. **Не всем давай номер телефона.** Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
9. **Выключай Bluetooth, когда не используешь его.** Иногда проверяй, не забыл ли выключить.

ПАМЯТКА 8.
Как безопасно играть online

Online – игры объединяют людей по всему миру. Игроки покупают диск, оплачивают абонемент или дополнительные опции. На эти средства совершенствуются системы авторизации, закрываются уязвимости. В играх стоит опасаться кражи пороля.

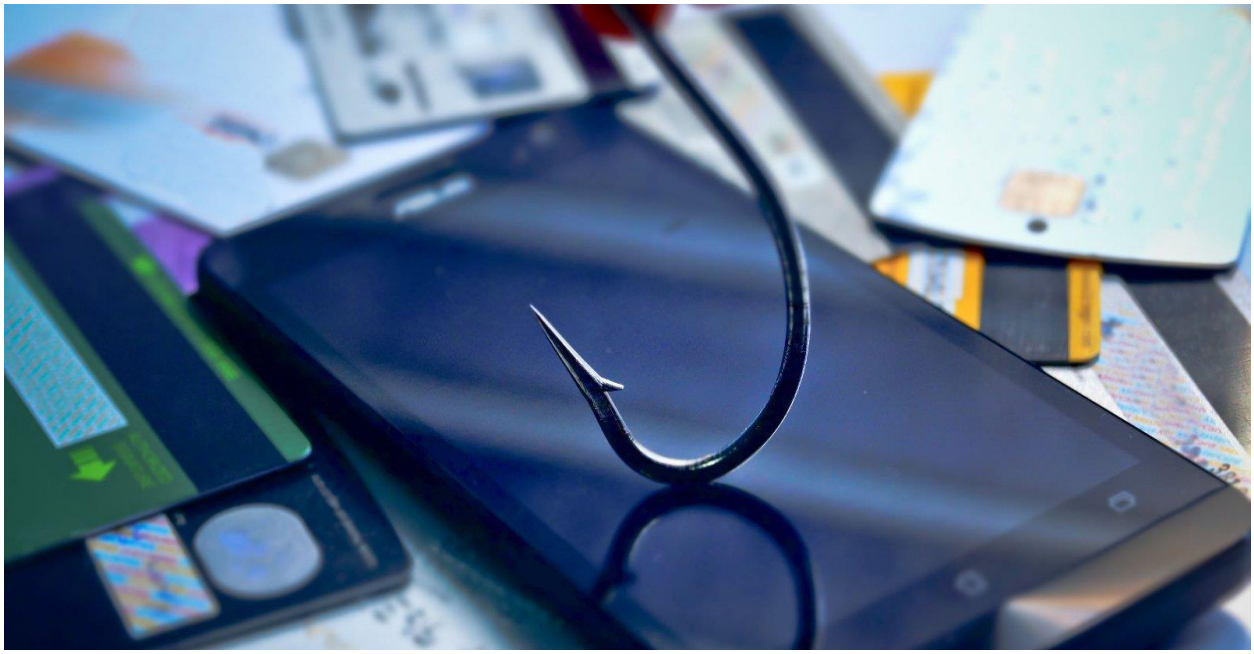
1. **Блокируй неадекватов.** Заблокируй в списке игроков того, кто ведет себя агрессивно по отношению к тебе или создает неприятности.
2. **Пожалуйся администраторам игры на поведение агрессивного игрока.** Желательно приложить доказательства в виде скринов.
3. **Будь осторожен.** Не указывай личную информацию в профайле игры.
4. **Следи за своим поведением.** Уважай других участников игры.
5. **Устанавливай проверенные утилиты.** Избегай неофициальных патчей и модов.
6. **Берегись взлома.** Используй сложные и разные пароли.
7. **Не отключай антивирус во время игры.** Пока ты играешь, твой компьютер могут заразить.



ПАМЯТКА 9.
Как защититься от фишинга.

ФИШИНГ – (от английского слова fishing – рыбная ловля) – вид интернет мошенничества.

1. **Следи за своим аккаунтом.** Если подозреваешь, что акаунт взломали, нужно заблокировать его или сообщить его администраторам ресурса об этом как можно скорее.
2. **Посещай только безопасные веб-**сайты. В их числе –сайты интернет – магазинов и поисковых систем.
3. **Используй сложные и разные пароли.** Если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в Сети, а не ко всем.
4. **Предупреди всех своих знакомых, которые добавлены у тебя в друзья, если тебя взломали.** От твоего имени могут рассылать спам и ссылки на фишшинговые сайты.
5. **Спрячь данные.** Установи надежный пароль (PIN) на мобильный телефон.
6. **Отключи сохранение пароля в браузере.** Сохраненные пароли крадут чаще.
7. **Не открывай файлы и другие вложения в письмах Даже если они пришли от твоих друзей.** Уточни у них, отправляли ли они тебе эти файлы.



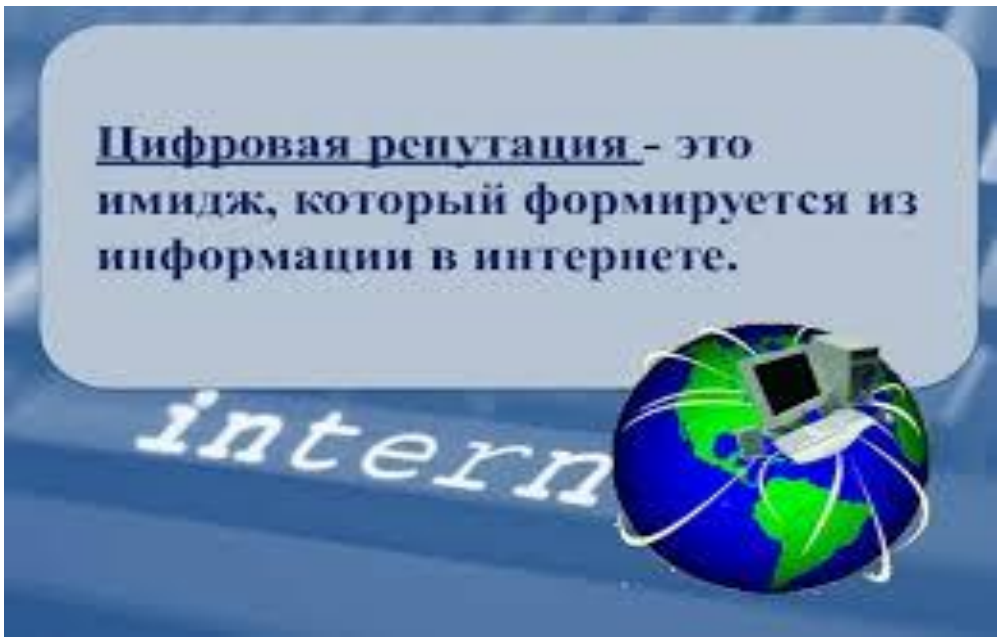
ПАМЯТКА 10.
Как защитить свою репутацию

ЦИФРОВАЯ РЕПУТАЦИЯ – это твой имидж, который формируется из информации о тебе в интернете. Компрометирующая информация в интернете может серьезно отразиться на реальной жизни. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Многие подростки легкомысленно относятся к публикации личной информации в интернете, не понимая возможных последствий. Ты даже не задумываешься о том, что фотография, размещения пять лет назад, может стать причиной отказа принять тебя на работу.

Комментарии, фотографии и твои действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она. Найти информацию много лет спустя сможет любой – как из добрых пробуждений, так и с намерением причинить вред.

Советы по защите цифровой репутации:

1. Не публикуй сразу. Подумай, прежде чем что-то публиковать у себя в блоге или в социальной сети, пересылать в личном сообщении.
2. Установки ограничения в настройках профиля. Ограничить просмотр профиля и его содержимого. Сделай его только «для друзей».
3. Берегись исков за оскорбление личности в интернете. Не размещай информацию, которая может кого-то обижать, и не ссылайся на нее.



ПАМЯТКА 11.
Что такое авторское право

Чтобы использовать возможности цифрового мира, нужно соблюдать права на интеллектуальную собственность. Термин интеллектуальная собственность относится к различным творениям человеческого ума, начиная с новых изобретении и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность – на произведения науки, литературы и искусства. Авторские права выступают как гарантия возможностей автора заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать или размещать в интернете.

«Пиратское» программное обеспечение несет в себе многие риски: от потери данных до блокировки устройства, где установлена нелегальная программа. Не забывайте, что в Сети найти легальные и бесплатные программы со сходным функционалом.